مقدمه
في
نظرية الأعداد

أ.د. فالح بن عمران بن محمد الدوسري
قسم العلوم الرياضية – كلية العلوم التطبيقية
جامعة أم القرى – مكة المكرمة

الطبعة الأولـــى
١٤٢٨هـ-٢٠٠٧م

المقدمة

الحمد لله الذي علّم بالقلم ، علّم الإنسان ما لم يعلم ، والصلاة والسلام على خاتم الأنبياء والمرسلين سيدنا وقدوتنا محمد (ﷺ) وعلى آله وصحبه أجمعين .

وبعد فالعدد لغة العلم ، وأفضل وسيله للتعبير عنه هي الرموز ، والأرقام هي أشكال تكتب بها رموز الأعداد ، والحساب أو نظرية الأعداد هو علم العدد ، جانبه النظري يعالج الأرقام والأعداد ، مراتبها والنسب التي بينها وتكرارها على نسق معين ، أنواعها وكيفية بنائها ودراسة خواصها والعلاقات بينها ، وجانبه العملي يتناول الحسبان ، معرفة المطلوب بالعمليات الأربعة ، وتكثر الحاجة إلى الحسبان بإستخراج المطلوب من صلة بعض الأشياء ببعض ولولا الحسبان لعجز الإنسان عن تسجيل أحداث الزمن ولما وجدت التقاويم والنقود ، ومما جاء عن ابن سراقة : أن الحساب علم قديم فوائده جمه منها ما في الميقات من أوقات الصلاة وحساب الأعوام والشهور والأيام وحركات الشمس في البروج والكواكب وحلول القمر في المنازل المقدرة له ومعرفة الساعات وغير ذلك ، ومنها في علم الفقه في حساب الزكاة وما يحسبه المكلف في الصيام وأعمال الحج وقسمة الغنائم والمساقاه والإجارة وغير ذلك مما يحتاج إليه غالب الناس ، ومنها ما في علم الفرائض من التأجيل والتصحيح وقسمة التركات، بل أن الله تعالي قال بحق نفسه " **وهو أسرع الحاسبين** " ولأهمية علم الحساب في حياة الناس اليومية جعله الجاحظ يشمل على معانٍ كثيرة ومنافع جليلة والجهل به فساد جل النعم وفقدان جمهور المنافع واختلال كل ما جعله الله عز وجل لنا قواماً ومصلحة ونظاماً ، وقال جاوس الرياضيات ملكة العلوم والحساب ملك الرياضيات ، وعليه ولقلة المراجع في هذا المجال ، نقدم هذا الكتاب الذي يضم ثمانية فصول يحتوي على أساسيات نظرية الأعداد وبعض تطبيقاتها ، ندرس في الفصل الأول منها خواص الأعداد الصحيحة والأستقراء الرياضي وقاعدة الترتيب الجيد . وقد بدأ الأستقراء

الرياضي مع الكرخي (ت١٠٢٠م) ، لأنه أول من أثبت بشكل من الأستقراء الرياضي أن $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ ، $\sum_{i=1}^{n} i^3 = (\sum_{i=1}^{n} i)^2$ ، أما كل من الحسن ابن الهيثم والسمؤال المغربي وابن البنا المراكشي ، فقد أثبت تلك العلاقات بطرق مختلفة ، أما العلاقة $\sum_{i=1}^{n} i^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$ ، فقد أثبت من قبل كل من أبو جعفر القبيصي أحد رياضي القرن العاشر للميلاد ، وأبو منصور عبد القادر البغدادي والحسن ابن الهيثم وغياث الدين الكاشي . أما قاعدة الترتيب الجيد فقد وضعت من قبل كانتور وزرملّو كإحدى طرق البرهان المكافئة للأستقراء الرياضي من جهة ولمسلمه الأختيار من جهة أخرى .

ونظراً لأهمية القسمة والقاسم المشترك الأعظم والمضاعف المشترك البسيط وكيفية إيجادهما ، الأعداد الأولية وخواصها والمبرهنة الأساسية في الحساب وتطبيقاتها ، خصّص الفصل الثاني لدراستها . أما في الفصل الثالث ، فندرس التطابقات ، التي تقدم مفهوماً آخراً للقسمة قدمت من قبل جاوس عام ١٨٠١م بطريقة جعلتها أداة فعالة لتسهيل البراهين ووسيلة آخرى لدراسة نظرية الأعداد وضم هذا الفصل خواص التطابق وفصوله وبعض تطبيقاته ، البواقي التامة والمختزلة والتطابقات الخطية ومبرهنة الباقي الصينية ، إضافة إلى مبرهنتي أويلر وفيرما ومبرهنة ابن الهيثم " ولسن " .

وندرس في الفصل الرابع الدوال العددية مثل القواسم وعددها لعدد صحيح والتي ظهرت في أبحاث أبو جعفر الخازن وأبو سعيد السجزي من رياضي القرن العاشر للميلاد ، ثم ندرس دالة أويلر وخواصها ، دالة موبيص والدالة زيتا .

وندرس في الفصل الخامس أنواعاً خاصة من الأعداد وهي أعداد فيرما ومرسين ، الأعداد التامة المعرفة من قبل إقليدس ، الأعداد المتحابة المعرفة من قبل فيثاغورس الأعداد المتعادلة المعرفة من قبل عبد القادر البغدادي .

أما في الفصل السادس فندرس الجذور البدائية التي وردت في أبحاث أويلر سنة ١٧٧٣م ولجندر سنة ١٧٨٥م وجاوس سنة ١٧٩٦م ، ثم ندرس البواقي

التربيعية وخواصها ورمز لجندر ، ثم قانون التعاكس لجاوس ، والذي خُمّن من قبل أويلر سنة ١٧٤٢م وبُرهن جزئياً من قبل لجندر سنة ١٧٨٥م ثم أثبت من قبل جاوس سنة ١٧٩٦م ونشر سنة ١٨٠١م .

أما الفصل السابع فيحتوي على بعض المعالات الديوفنتية مثل المعادلات الديوفنتية الخطية التي بدأت مع ديوفنتس وطورت من قبل ابن أسلم المصري والكرخي والسمؤال المغربي والخازن والسجزي ثم فيرما وأويلر ، أما المعادلة $x^2 + y^2 = z^2$ وثلاثيات فيثاغورس أو ما يسمى المثلثات العددية قائمة الزاوية ، فقد بدأت مع البابلين والمصريين ، ثم فيثاغورس ، أبو جعفر الخازن أحد رياضي القرن العاشر للميلاد، أما في البند الثالث من هذا الفصل فقد درست بعض الحالات الخاصة لمبرهنة فيرما الأخيرة والتي تعتبر من أهم وأشهر المبرهنات في نظرية الأعداد ، والتي تنص على عدم وجود أعداد صحيحة غير صفرية تحقق العلاقة $x^n + y^n = z^n$ ، $n \geq 3$.
مؤكدين على تعامل الرياضيين المسلمين أمثال الكرخي والخجندي والخازن والخيام وابن سينا مع الحالتين الخاصتين $x^4 + y^4 = z^4$ ، $x^3 + y^3 = z^3$. وأخيراً ندرس كيفية التعبير عن عدد طبيعي كمجموع مربعين أو أكثر والتي بدأت مع ديوفنتس وتطورت مع الخازن وباشيه وفيرما ، لاجرانج وأويلر .

ونظراً لأهمية الكسور المستمرة ، لعلاقتها بالأعداد الحقيقية من جهة وكثرة تطبيقاتها من جهة أخرى خصص الفصل الأخير لدراسة هذا النوع من الكسور والذي ظهر في أبحاث الإيطاليين بومبللي سنة ١٥٧٢م ، كاتالدي سنة ١٦١٣م ، الإنجليزي جون وايلس سنة ١٦٥٣م وأويلر ولاجرانج وجاوس .

وأخيراً أود أن أشكر زميلي الأخ الدكتور محمود بن عبد القادر خليفة على مساعدته لي في الحصول على بعض المراجع ، سائلاً الله العلي القدير إن يرحمنا ويرحم والدينا ويجعل أعمالنا خالصة لوجه الكريم ، وآخر دعوانا إن الحمد لله رب العالمين ،،،

٢٧ ربيع الأول ١٤٢٨هـ
١٥ إبريل ٢٠٠٧م

المحتوى

الفصل الأول

مفاهيم أساسية (Basic Concepts)

يضم هذا الفصل بندان تناولنا فيهما بعض خواص الأعداد الصحيحة وقاعدتي الإستنتاج (الأستقراء) الرياضي والترتيب الجيد .

١-١ : خواص الأعداد الصحيحة

يمكن بناء الأعداد الصحيحة $Z=\{0,\mp1,\mp2,\cdots\}$ من مجموعة الأعداد الطبيعية $N=\{0,1,2,3,\cdots\}$ ، وإثبات خواص جمعها وضربها كما في [١]، لكننا سنورد تلك الخواص دون إثبات لأي منها ، ثم نستنتج منها خواصاً أساسية أخرى .

فإذا كان $a,b,c\in Z$ ، فإن :

(١) $a+b=b+a$ ، $a\cdot b=b\cdot a$. أي أن جمع وضرب الأعداد الصحيحة إبدالي (تبديلي Commutative) .

(٢) $(a+b)+c=a+(b+c)$ ، $(a\cdot b)\cdot c=a\cdot(b\cdot c)$. أي أن جمع وضرب الأعداد الصحيحة تجميعي (Associative) .

(٣) $a+0=0+a=a$ ، $a\cdot1=1\cdot a=a$.

(٤) لكل $a\in Z$ ، يوجد $-a\in Z$ بحيث أن $a+(-a)=(-a)+a=0$.

(٥) $a\cdot(b+c)=a\cdot b+a\cdot c$ ، $(a+b)\cdot c=a\cdot c+b\cdot c$ أي أن الضرب توزيعي على الجمع .

(٦) إذا كان $a+b=a+c$ ، فإن $b=c$.

(٧) لكل $a,b\in N$ ، نجد أن $a+b\in N$ ، $a\cdot b\in N$.

والآن إلى المبرهنة الآتية :

مبرهنة ١-١-١ : إذا كان $a,b \in Z$ فإن

(أ) $a \cdot 0 = 0 \cdot a = 0$ ، (ب) $(-a) \cdot b = a(-b) = -(ab)$

(ج) $-(-a) = a$ ، (د) $(-a)(-b) = ab$

البرهان :

(أ) بما أن $0 + 0 = 0$. إذاً $a \cdot (0+0) = a \cdot 0$ ، وعليه فإن $a \cdot 0 + a \cdot 0 = a \cdot 0$ لكن $a \cdot 0 = a \cdot 0 + 0$. إذاً $a \cdot 0 + a \cdot 0 = a \cdot 0 + 0$ ، وعليه فإن $a \cdot 0 = 0$ (حسب الخاصية ٦) . لكن $a \cdot 0 = 0 \cdot a$ (حسب الخاصية ١) . إذاً $a \cdot 0 = 0 \cdot a = 0$.

(ب) بما أن $(-a) \cdot b = (-a) \cdot b + 0$ (حسب الخاصية ٣) . وبما أن $ab + (-(ab)) = 0$ (حسب الخاصية ٤) . إذاً باستخدام الخواص (٢)،(٣)،(٥) نجد أن

$$(-a) \cdot b = (-a)b + [ab + (-(ab))] = [(-a)b + ab] + (-(ab))$$
$$((-a) + a)b + (-(ab)) = 0 \cdot b + (-(ab)) = 0 + (-(ab)) = -(ab)$$

وبنفس الطريقة يمكن أن نبرهن على أن $a(-b) = -(ab)$. إذاً $(-a)b = a(-b) = -(ab)$.

(ج) بما أن $-(-a) = -(-a) + 0$ و $(-a) + a = 0$. إذاً

$$-(-a) = -(-a) + [(-a) + a] = [-(-a) + (-a)] + a = 0 + a = a$$

(د) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$ حسب (ب ، ج) .

□

تعريف ١-١-١ :

إذا كان $N^* = N - \{0\} = \{1,2,3,\cdots\} = Z^+$ وكان $a,b \in Z$ فيقال عن

(أ) a أنها أصغر من b أو أن b أكبر من a ونكتب $a < b$ إذا كان

$$b - a \in N^*$$

(ب) a أنها أصغر أو تساوي b أو أن b أكبر أو تساوي a ونكتب $a \le b$ إذا كان $b-a \in N$.

مبرهنة ١-١-٢ :

(أ) إذا كان $a,b,c \in Z$ وكان $a<b$ و $b<c$ فإن $a<c$.

(ب) إذا كان $a,b,c \in Z$ ، $a<b$ ، $c>0$ ، فإن $ac<bc$.

(ج) إذا كان $a,b \in Z$ فواحدة فقط مما يأتي صحيحة : إما $a<b$ أو $a=b$ أو $a<b$.

البرهان :

(أ) بما أن $a<b \Leftrightarrow b-a \in N^*$ ، $b<c \Leftrightarrow c-b \in N^*$ إذاً $(c-b)+(b-a) \in N^*$ ، وعليه فإن $c-a \in N^*$ ومنه ينتج أن $a<c$.

(ب) بما أن $a<b \Leftrightarrow b-a \in N^*$ وبما أن $c \in N^*$ إذاً $(b-a)c = bc-ac \in N^*$ ، وعليه فإن $ac<bc$.

(ج) نفرض أن $a<b$ و $a=b$. إذاً $b<b$ وهذا تناقض . وإذا كان $a>b$ و $a=b$. فإن $b>b$ وهذا تناقض أيضاً . أما إذا كان $a<b$ و $a>b$ فإن $a<a$ حسب (أ) وهذا تناقض أيضاً . إذاً واحدة فقط من العبارات أعلاه صحيحة .

□

تعريف ١-١-٢ :

إذا كان $a \in Z$ فيقال عن $|a|$ أنها القيمة المطلقة (Absolute vatue) للعدد a إذا كان

$$|a| = \begin{cases} a & \forall a \ge 0 \\ -a & \forall a < 0 \end{cases}$$

مبرهنة ١-١-٣ : إذا كان $a,b\in Z$ ، فإن

(أ) $|a|\geq 0$ ، (ب) $|a|=0\Leftrightarrow a=0$ ، (ج) $-|a|\leq a\leq |a|$

(د) $|-a|=|a|$ ، (هـ) $|ab|=|a|\,|b|$ ، (و) $|a|\leq b\Leftrightarrow -b\leq a\leq b$

(ز) $|a+b|\leq |a|+|b|$ ، (ح) $|a-b|\geq |a|-|b|$

البرهان : سنثبت أ ، ج ، هـ ، ز

(أ) إذا كان $a\geq 0$ ، فإن $|a|=a\geq 0$. وإذا كان $a<0$ ، فإن $|a|=-a>0$ إذاً $|a|\geq 0$.

(ج) نفرض أن $a\geq 0$. إذاً $|a|=a$ ، وعليه فإن $|a|\geq 0$ ومنه ينتج أن $-|a|\leq 0$. إذاً $-|a|\leq 0\leq a=|a|$ وعليه فإن $-|a|\leq a\leq |a|$. أما إذا كان $a<0$ ، فإن $-a>0$ وعليه فإن $|a|=-a>0$ ومنه ينتج أن $-|a|<0$. إذاً $-|a|=a<0<-a=|a|$ وعليه فإن $-|a|\leq a\leq |a|$.

(هـ) إذا كان $a\geq 0$ ، $b\geq 0$ ، فإن $ab\geq 0$ وعليه فإن $|a|=a$ ، $|b|=b$ ومنه ينتج أن $|ab|=ab=|a|\,|b|$. وإذا كان $a\geq 0$ ، $b<0$ ، فإن $ab<0$ ، وعليه فإن $|a|=a$ ، $|b|=-b$. إذاً $|ab|=a(-b)=|a|\,|b|$. وإذا كان $a<0$ ، $b\geq 0$ ، فإن $ab<0$ و $|a|=-a$ و $|b|=b$ ، وعليه فإن $|ab|=-(ab)=(-a)b=|a|\,|b|$. وإذا كان $a<0$ ، $b<0$ ، فإن $ab>0$ ، $|a|=-a$ ، $|b|=-b$ ، وعليه فإن $|ab|=ab$ ومنه ينتج أن $|ab|=|a|\,|b|$

(ز) بما أن $-|a|\leq a\leq |a|$ و $-|b|\leq b\leq |b|$ حسب (ج) . إذاً $-\left(|a|+|b|\right)\leq a+b\leq |a|+|b|$ وحيث أن $a,b\in Z$. إذاً إما $a+b\geq 0$ أو $a+b<0$ فإذا كان $a+b\geq 0$ ، فإن $|a+b|=a+b$ وعليه فإن $|a+b|\leq |a|+|b|$ أما إذا كان $a+b<0$ ، فإن $|a+b|=-(a+b)$. لكن $-\left(|a|+|b|\right)\leq a+b$. إذاً $|a|+|b|\geq -(a+b)$ ، وعليه فإن $|a+b|\leq |a|+|b|$.

١-٢ : قاعدة الترتيب الجيد والاستنتاج (الأستقراء) الرياضي

Well-ordering principle and Mathematical Induction

سنركز اهتمامنا في هذا الجزء على قاعدة الترتيب الجيد وعلاقتها بالأستنتاج الرياضي ، ونبدأ بالآتي :

تعريف ١-٢-١ :

يقال عن علاقة $\preceq$ على مجموعة غير خالية A أنها علاقة ترتيب جزئي (partial order relation) إذا كانت :

(أ) $\preceq$ علاقة منعكسة (reflexive) على A . أي أن $a \preceq a$ لكل $a \in A$.

(ب) $\preceq$ علاقة متخالفة أو تخالفيه (Antisymmetric) على A . أي أنه إذا كان $a \preceq b$ و $b \preceq a$ فإن $a = b$.

(ج) $\preceq$ علاقة متعدية(transitive) على A. أي أنه إذا كان $a \preceq b$ و $b \preceq c$ ، فإن $a \preceq c$.

ويقال عن $(A, \preceq)$ أنها مجموعة مرتبة ترتيباً جزئياً (partially ordered set) ، إذا كانت $A \neq \varnothing$ و $\preceq$ علاقة ترتيب جزئي على A .

مثال ١-٢-١ :

(أ) إذا كان $A \in \{N, Z, Q, R\}$ ، وكان $a \preceq b \Leftrightarrow a \leq b$ فإن $(A, \preceq)$ مجموعة مرتبة ترتيباً جزئياً .

(ب) إذا كانت $X \neq \varnothing$ ، فإن $(P(X), \subseteq)$ مجموعة مرتبة ترتيباً جزئياً لأن $P(X) \neq \varnothing$ و $\subseteq$ علاقة ترتيب جزئي على P(X) .

(ج) إذا كانت $A = \{1,2,3,4\}$ ،

$$\preceq = \{(1,1), (2,2), (3,3), (4,4)\ (1,2), (2,3), (1,3), (2,4), (1,4)\}$$

، فإن $\preceq$ علاقة ترتيب جزئي على A .

(د) إذا كانت $\preceq$ معرفة على N^* كالآتي : $a \preceq b \Leftrightarrow b \setminus a$ ، فإن $\preceq$ علاقة ترتيب جزئي على N^* ، وعليه فإن $(N^*, \preceq)$ مجموعة مرتبة ترتيباً جزئياً .

تعريف ١-٢-٢ :

إذا كانت $(A,\preceq)$ مجموعة مرتبة ترتيباً جزئياً ، فيقال عن $a \in A$ أنه عنصر أول أو عنصر أصغر(first or least or smallest element) للمجموعة A ونكتب $l(A)=a$ إذا كان $a \preceq x$ لكل $x \in A$.

مثال ١-٢-٢ :

(أ) $(N\ ,\le)$مجموعة مرتبة ترتيباً جزئياً ، $l(N)=0$.

(ب) إذا كانت $X \neq \varnothing$ ، فإن $(P(X),\subseteq)$ مجموعة مرتبة ترتيباً جزئياً ، $l(P(X))=\varnothing$ ، لأن $\varnothing \subseteq A$ لكل $A \in P(X)$.

(ج) إذا كانت $A=\{x \in R \mid 0<x<1\}$ ، فإن $(A,\le)$ مجموعة مرتبة ترتيباً جزئياً لكنها لا تملك عنصر أول .

(د) إذا كانت $A=\{2,4,6\}$ وكانت $\preceq$ معرفة على A كالآتي : $a,b \in A\ ,\ a \preceq b \Leftrightarrow a \backslash b$ ، إذاً $(A,\preceq)$ مجموعة مرتبة ترتيباً جزئياً و $l(A)=2$.

تعريف ١-٢-٣ :

يقال عن مجموعة مرتبة ترتيباً جزئياً $(A,\preceq)$ أنها مجموعة مرتبة ترتيباً جيداً (well-ordered Set) إذا كانت كل مجموعة جزئية غير خالية من A تحوي عنصراً أولاً .

مثال ١-٢-٣ :

(أ) إذا كانت $A=\{1,2,3,4\}$ ، فإن $(A,\le)$ مجموعة مرتبة ترتيباً جيداً لأن $(A,\le)$ مجموعة مرتبة ترتيباً جزئياً وكل مجموعة جزئية من A تحوي عنصر أول .

(ب) إذا كانت $A=\{1,2,4,8\}$ ، $a \preceq b \Leftrightarrow a \setminus b$ فإن $(A,\leq)$ مجموعة مرتبة ترتيباً جيداً لأن $(A,\leq)$ مجموعة مرتبة ترتيباً جزئياً وكل مجموعة جزئية تحوي عنصر أول .

(ج) لكل $n \in N$ ، نجد أن $A=(\{r \in N \mid r<n\},\leq)$ مجموعة مرتبة ترتيباً جيداً .

(د) إذا كانت $A=[0,1]$ فإن A مجموعة ليست مرتبة ترتيباً جيداً لأن $B=]0,1] \underset{\neq}{\subset} A$ لا تحوي عنصر أول .

(هـ) إذا كانت $A=N^2$ ، $\preceq$ معرفة A كالآتي :

إذا كانت $(a,b),(c,d) \in A$ فإن

$2^d(2a+1) \leq 2^b(2c+1) \Leftrightarrow (a,b) \preceq (c,d)$ فإن $(A,\leq)$ مجموعة ليست مرتبة ترتيباً جيداً لأن $(a,b+1) \leq (a,b)$ لكل $a,b \in N$ ، وعليه إن A لا تملك عنصر أول .

(و) $(Z,\leq)$ مجموعة ليست مرتبة ترتيباً جيداً ، لأن $\{\cdots,-3,-2,-1\}$ مجموعة جزئية منها لا تحوي على عنصر أول (عنصر أصغر) .

قاعدة الترتيب الجيد (Well-ordering principle)

$(N,\leq)$ مجموعة مرتبة ترتيباً جيداً .

والآن إلى المبرهنة الآتية التي تبين بعض تطبيقات قاعدة الترتب الجيد .

مبرهنة ١-٢-١ :

(أ) لا يوجد عدد صحيح بين الصفر والواحد .

(ب) الواحد أصغر عدد موجب .

(ج) إذا كان $n \in Z$ ، فلا يوجد $m \in Z$ ، بحيث أن $n<m<n+1$.

البرهان :

(أ) نفرض وجود $x \in N$ بحيث أن $0 < x < 1$. إذاً $S = \{ m \in N | 0 < m < 1 \} \neq \varnothing$. لكن N مرتبة جيداً ، $\varnothing \neq S \subseteq N$. إذاً S تملك عنصر أول (أصغر) وليكن n . إذاً $0 < n < 1$ ، وعليه فإن $0 < n^2 < n < 1$ ، وهذا يعني أن $n^2 \in S$ و $n^2 < n$ وهذا يناقض كون n عنصر أول في S . إذاً $S = \varnothing$.

(ب) بما أن $S = \{ m \in N | 0 < m < 1 \} = \varnothing$ حسب (أ) . إذاً الواحد هو أصغر عدد صحيح موجب .

(ج) نفرض وجود $m \in Z$ بحيث أن $n < m < n + 1$. إذاً $0 < (m - n) < 1$ وهذا يناقض (أ). إذاً لا يوجد $m \in Z$ بحيث أن $n < m < n + 1$

□

ولتوضيح العلاقة بين قاعدة الترتيب الجيد والأستقراء الرياضي نورد المبرهنة الآتية :

مبرهنة ١-٢-٤: العبارات الآتية متكافئة .

(أ) قاعدة الأستقراء الرياضي (principle of Mathematical Induction)
إذا كانت B مجموعة جزئية من N^* وكان $1 \in B$ و $(n \in B \Rightarrow n + 1 \in B)$ فإن $B = N^*$.

(ب) القاعدة العامة للأستقراء الرياضي (Transfinite Induction) .
إذا كانت B مجموعة جزئية من N^* ، وكان $1 \in B$ و ($n \in B$ عندما $m \in B$ لكل $m < n$) ، فإن $B = N^*$.

(ج) لكل مجموعة جزئية غير خالية من N^* عنصر أول (أصغر) .

البرهان : سنثبت أن (أ) ⇐ (ب) ⇐ (ج) ⇐ (أ) .

(أ) ⇐ (ب) لتكن $B \subseteq N$ بحيث أن $1 \in B$ و ($n \in B$ عندما $m \in B$ لكل $m < n$) . ولنفرض $E = \{ x \in N | y \in B \; \forall \; y \leq x \}$. إذاً $E \subseteq B$ وعليه يتم المطلوب إذا أثبتنا أن $E = N^*$.

ولإثبات ذلك لاحظ أن $1 \in E$ لأن $1 \in B$ وإذا كان $n \in E$ ، فإن $y \in B$ لكل $y \le n$. إذاً $(n+1) \in B$ وعليه فإن $y \in B$ لكل $y \le n+1$ وهذا يعني أن $n+1 \in E$. إذاً $E = N^*$ حسب (أ) .

(ب) $\Leftarrow$ (ج) لتكن B مجموعة جزئية من N^* و B لا تملك عنصر أول . إذاً $1 \notin B$ وعليه فإن $1 \in N^* - B$. إذا كانت $m \in N^* - B$ لكل $m < n$ ، فإن $n \in N^* - B$ لأنه إذا كان العكس فإن n هي العنصر الأول للمجموعة B وهذا يناقض الفرض. إذاً $N^* - B = N^*$ حسب (ب) ومنه ينتج أن $B = \varnothing$. إذاً لكل مجموعة جزئية غير خالية من N^* عنصر أول

(ج) $\Leftarrow$ (أ) لتكن B مجموعة جزئية من N^* بحيث أن $1 \in B$ و $(n \in B \Rightarrow n+1 \in B)$ ولتكن $B' = N^* - B$ إذاً إذا كانت $B' \neq \varnothing$ ، فإن B' تملك عنصر أول وليكن m . إذاً $m \neq 1$ لأن $1 \in B$ وعليه فإن $m > 1$. لكن $m - 1 < m$. إذاً $(m-1) \notin B'$ ، وعليه فإن $m - 1 \in B$ ، وبالتالي فإن $m = (m-1) + 1 \in B$. إذاً $m \notin B'$ وهذا تناقض . إذاً $B' = \varnothing$ وعليه فإن $B = N^*$.

□

ملاحظة :

لإثبات صحة العبارة $P(n)$ لجميع قيم $n \in N^*$ يكفي أن نبرهن على أن $P(1)$ عبارة صحيحة ونثبت أن صدق العبارة $P(m)$ يؤدي إلى صدق العبارة $P(m+1)$ ، لأنه إذا كانت $S = \{n \in N^* \mid P(n)$ عبارة صحيحة $\}$ ، فإن $1 \in S$ ، كما أنه إذا كان $m \in S$ فإن $m + 1 \in S$ ، وعليه فإن $S = N^*$.

مثال (١) :

أثبت أن $$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

أن أول من أثبت صحة تلك العلاقة هو أبو بكر الكوخي ، أما الحسن بن الهيثم والسموءل المغربي وابن البناء المراكشي فقد أثبتوها بطرق مختلفة ، أنظر [٣] .

الإثبات :

نفرض أن $P(n)\equiv\sum_{i=1}^{n}i^2=\frac{n(n+1)(2n+1)}{6}$ ، إذاً عندما $n=1$ نجد أن الطرف الأيمن $=\frac{1\times2\times3}{6}=1$ ، والطرف الأيسر $=1^2=1$ أيضاً وعليه فإن $P(1)$ عبارة صادقة .

والآن أفرض أن $P(m)$ عبارة صادقة . نجد أن

$$\sum_{i=1}^{m}i^2=\frac{m(m+1)(2m+1)}{6}$$

ولإثبات صحة العبارة $P(m+1)$ لاحظ أن

$$\sum_{i=1}^{m}i^2+(m+1)^2=\frac{m(m+1)(2m+1)}{6}+(m+1)^2$$

وعليه فإن

$$\sum_{i=1}^{m-1}i^2=\frac{(m+1)\left[m(2m+1)+6(m+1)\right]}{6}=\frac{(m+1)[2m^2+7m+6]}{6}$$

$$=\frac{(m+1)(m+2)(2m+3)}{6}=\frac{(m+1)\left[(m+1)+1\right]\left[2(m+1)+1\right]}{6}$$

إذاً $P(m+1)$ عبارة صادقة ، وعليه فإن $P(n)$ عبارة صادقة لجميع قيم n الصحيحة الموجبة .

مثال (٢) :

إذا كان a,b عددين حقيقين، $n\in N^*$ ، فأثبت أن

$$\frac{a^n-b^n}{a-b}=\sum_{i=1}^{n}a^{n-i}b^{i-1}$$

الإثبات :

نفرض أن $P(n):\frac{a^n-b^n}{a-b}=\sum_{i=1}^{n}a^{n-i}b^{i-1}$. إذاً عندما $n=1$ نجد أن $L.H.S.=1$ ، $R.H.S.=\sum_{i=1}^{1}a^{1-i}b^{i-1}=1$ ، وعليه فإن الطرفين متساويان ، وبالتالي فإن $P(1)$ عبارة صادقة (صحيحة) .

والآن لنفرض أن $P(m)$ عبارة صـــادقة . إذاً $\frac{a^{m+1}-b^{m+1}}{a-b}=\sum_{i=1}^{m} a^{m-i} b^{i-1}$

ولإثبات صحة $P(m+1)$ ، لاحظ أن

$$\frac{a^{m+1}-b^{m+1}}{a-b}=\frac{a^{m+1}-ab^{m}+ab^{m}-b^{m+1}}{a-b}=a(\frac{a^{m}-b^{m}}{a-b})+b^{m}$$

$$=a\cdot\sum_{i=1}^{m} a^{m-i} b^{i-1}+b^{m}=a\left(a^{m-1}+a^{m-2}b+\cdots+ab^{m-2}+b^{m-1}\right)+b^{m}$$

$$=a^{m}+a^{m-1}b+\cdots+ab^{m-1}+b^{m}=\sum_{i=1}^{m+1} a^{(m+1)-i} b^{i-1}$$

وعليه فإن $P(m+1)$ صادقة وبالتالي فإن $P(n)$ صادقة لكل $n\in N^{*}$.

<u>**مثال (٣) :**</u> أثبت أن

$$a+(a+r)+(a+2r)+\cdots+[a+(n-1)r]=\frac{n}{2}[2a+(n-1)r]$$

لاحظ أن الطرف الأيسر يمثل متتابعة عددية حدها الأول a وأساسها r ، وعدد حدودها n . وأول من أثبت صحة تلك العلاقة أبا بكر فخـــر الـــدين الكرخـــي المتوفي عام ٤٢١هـــ .

<u>**الإثبات :**</u>

لـــــتكن $P(n):a+(a+r)+(a+2r)+\cdots+[a+(n-1)r]=\frac{n}{2}[2a+(n-1)r]$.

فإذا كان $n=1$ فإن $L.H.S.=a$ ، $R.H.S.=a$ وعليه فإن $P(1)$ صحيحة .

نفرض أن $P(m)$ صحيحة إذاً

$$a+(a+r)+(a+2r)+\cdots+[a+(m-1)r]=\frac{m}{2}[2a+(m-1)r]$$

وعليه فإن

$$a+(a+r)+(a+2r)+\cdots+[a+(m-1)r]+(a+mr)$$

$$=\frac{m}{2}[2a+(m-1)r]+(a+mr)$$

$$a+(a+r)+(a+2r)+\cdots+(a+mr)=(m+1)a+\frac{[m(m-1)+2m]\cdot r}{2}$$

$$=(m+1)a+\frac{m(m+1)r}{2}=\frac{m+1}{2}(2a+mr)$$

وعليه فإن $P(m+1)$ صحيحة . إذاً $P(n)$ صحيحة لكل $n\in Z^*$.

مثال (٤) :

إذا كان $ab=ba$ ، فإن $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$ لكل $n\in N^*$ ، حيث $\binom{n}{k}=\frac{n!}{k!(n-k)!}$. يسمى هذا القانون " مبرهنة ذي الحدين " والتي يجب أن تنسب إلى أبي بكر الكرخي .

الإثبات :

لتكن $P(n):(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$. إذاً إذا كانت $n=1$ ، فإن

$$R.H.S.=\sum_{k=0}^{1}\binom{1}{k}a^{1-k}b^k=\binom{1}{0}a+\binom{1}{1}b=a+b \text{ ، } L.H.S.=a+b$$

وعليه فإن $P(1)$ صحيحة . والآن لنفرض أن $P(m)$ ، إذاً

$(a+b)^m=\sum_{k=0}^{m}\binom{m}{k}a^{m-k}b^k$ ، وعليه فإن

$$(a+b)^{m+1}=\sum_{k=0}^{m}\binom{m}{k}a^{m-k}b^k(a+b)$$

$$=\left[\binom{m}{0}a^m+\binom{m}{1}a^{m-1}b+\binom{m}{2}a^{m-2}b^2+\cdots+\binom{m}{m}b^m\right](a+b)$$

$$=\binom{m}{0}a^{m+1}\left[\binom{m}{0}+\binom{m}{1}\right]a^mb+\cdots+\left[\binom{m}{i}+\binom{m}{i-1}\right]a^{m+1-i}b^i+\cdots+\binom{m}{m}b^{m+1}$$

لكن $\binom{m}{k}+\binom{m}{k-1}=\binom{m+1}{k}$ ، إذاً

$$(a+b)^{m+1}=\binom{m+1}{0}a^{m+1}+\cdots+\binom{m+1}{i}a^{m+1-i}b^{i}+\cdots+\binom{m+1}{m+1}b^{m+1}$$
$$=\sum_{k=0}^{m+1}\binom{m+1}{k}a^{(m+1)-k}b^{k}$$

إذاً $P(m+1)$ صحيحة . وعليه فإن $P(n)$ صحيحة لكل $n\in Z^{*}$.

مثال (٥): متتابعة فيبوناشي (Fibonacci Sequence)

تنسب المتتابعة $1,1,2,3,5,8,13,21,34,\cdots$ إلى الايطالي ليوناردو فيبوناشي (١١٧٠ – ١٢٥٠م) ، الذي نقل في كتابة (Liber Abaci) الأرقام العربية إلى أوربا عام ١٢٠٢م ، ويقول البعض أن تلك المتتابعة معروفة من قبل وتعرّف كالآتي :

$f_1=f_2=1$ ، $f_{n+2}=f_{n+1}+f_n$ لكل $n\in N^{*}$.

أثبت أن

(أ) كلاً من f_{3n-1} ، f_{3n-2} عدد فردى بينما f_{3n} عدد زوجي لكل $n\in N^{*}$.

(ب) $f_{n+1}^{2}-f_n f_{n+2}=(-1)^{n}$ لكل $n\in N^{*}$.

البرهان : (بالإستقراء الرياضي على n)

(أ) إذا كان $n=1$ ، فإن $f_{3n-2}=f_1=1$ ، $f_{3n-1}=f_2=1$ بينما $f_{3n}=f_3=2$. إذاً عندما $n=1$ نجد أن كلاً من f_{3n-1} ، f_{3n-2} عدد فردي بينما f_{3n} عدد زوجي .

والآن لنفرض أن العبارة صحيحة (صادقة) عندما $n=m$ ، إذاً كل من f_{3m-1} ، f_{3m-2} عدد فردي بينما f_{3m} عدد زوجي . ولإثبات صحة العبارة عندما $n=m+1$ ، لاحظ أن $f_{3(m+1)-2}=f_{3m+1}=f_{3m}+f_{3m-1}$ حسب

تعريف متتابعة فيبوناشي لكن f_{3m} عدد زوجي ، f_{3m-1} عدد فردي بالفرض، ومجموع عددين أحدهما فردي والآخر زوجي يكون عدداً فردياً. إذاً f_{3m+1} عدد فردي . وحيث أن

$f_{3(m+1)-1} = f_{3m+1} = f_{3m+1} + f_{3m}$ و f_{3m+1} عدد فردي، f_{3m} عدد زوجي إذاً f_{3m+2} عدد فردي . وحيث أن

$f_{3(m+1)} = f_{3m+3} = f_{3m+2} + f_{3m+1}$ حسب تعريف متتابعة فيبوناشي لكن كلاً من f_{3m+1} ، f_{3m+2} عدد فردي ، كما أثبتنا ، إذاً f_{3m+3} عدد زوجي وعليه فإن العبارة أعلاه صحيحة عندما $n = m+1$ ، وبالتالي فإن كلاً من f_{3n-1} ، f_{3n-2} عدد فردي بينما f_{3n} عدد زوجي لكل $n \in N^*$.

(ب) نفرض أن $P(n): f_{n+1}^2 - f_n f_{n+2} = (-1)^n$. إذاً عندما $n = 1$ نجد أن $L.H.S = f_2^2 - f_1 f_3 = 1^2 - 1(2) = -1$ ، $R.H.S = (-1)^1 = -1$ ، وعليه فإن الطرفين متساويان وبالتالي فإن $P(1)$ صحيحة .

والآن لنفرض أن $P(m)$ صحيحة . إذاً $f_{m+1}^2 - f_m f_{m+2} = (-1)^m$ ، ولإثبات صحة $P(m+1)$ ، لاحظ أن

$f_{m+3} = f_{m+2} + f_{m+1}$ ، $f_{m+2} = f_{m+1} + f_m$ حسب تعريف متتابعة فيبوناشي ، وبالتالي فإن

$$\begin{aligned} f_{m+2}^2 - f_{m+1} f_{m+3} &= f_{m+2}^2 - f_{m+1}(f_{m+2} + f_{m+1}) \\ &= f_{m+2}^2 - f_{m+1} f_{m+2} - f_{m+1}^2 \\ &= f_{m+2}(f_{m+2} - f_{m+1}) - f_{m+1}^2 = f_{m+2} f_m - f_{m+1}^2 \\ &= -\left(f_{m+1}^2 - f_{m+2} \cdot f_m\right) = -(-1)^m = (-1)^{m+1} \end{aligned}$$

إذاً $P(m+1)$ صحيحة ، وعليه فإن $P(n)$ صحيحة لكل $n \in N^*$.

□

والآن إلى المبرهنة الآتية التي توضح بأنه قد يكون من المفيد أحياناً إثبات صحة علاقة لكل $a \geq b$.

مبرهنة ١-٢-٣ : العبارتان الآتيتان متكافئتان

(أ) قاعدة الإستنتاج (الأستقراء) الرياضي .

(ب) لتكن $b \in Z$ ، $S \subseteq T = \{ a \in Z | a \geq b \}$ بحيث أن $b \in S$ وإذا كان $n \in S$ فإن $n+1 \in S$ ، فإن $S = T$.

البرهان :

(أ) $\Leftarrow$ (ب)

لتكن $E = \{ a \in Z | a \in E \Leftrightarrow (a-1)+b \in S \}$. إذاً $1 \in E$ ، لأن $(1-1)+b = b \in S$. وحيث أن $\forall a \in E \ , (a-1)+b \in S \Rightarrow a \geq 1$. إذاً $n+1 \in E$ ، وعليه فإن $E = N^*$ حسب قاعدة الأستقراء الرياضي ، وبالتالي فإن $n \in E$ لكل $n = N^*$ ، وعليه فإن $(n-1)+b \in S$ لكل $n \in N^*$ لكن أي $a \geq b$ يمكن التعبير عنه بالشكل $a = (n-1)+b$ ، $a \in T$ إذاً $T \subseteq S$ ، وعليه فإن $S = T$.

(ب) $\Leftarrow$ (أ)

لتكن $E \subseteq N^*$ تحقق فرضيتي الأستقراء الرياضي ، ولكي نثبت أن $E = N^*$ نفرض أن S مجموعة معرفة كالآتي : $a \in S \Leftrightarrow a-b+1 \in E$ إذاً $b \in S$ ، لأن $(b-b)+1 = 1 \in E$ ، لكن $a \geq b \Leftrightarrow a-b+1 \in E$ فإذا فرضنا أن $a \in S$ ، فإن $a-b+1 \in E$ ، وعليه فإن $a-b+2 \in E$ وبالتالي فإن $a+1 \in S$ ، إذاً $S = \{ a \in Z | a \geq b \}$ حسب (ب) . لكن أي عدد صحيح موجب m يمكن التعبير عنه بالشكل $m = (r-b)+1$ ، $r \geq b$. إذاً $1 \leq m \in E$ ، وعليه فإن $E = N^*$.

□

مثال (٦):

أثبت أن (أ) $2^n > n$ لكل $n = N^*$

(ب) $2^n > 5n$ لكل $n \geq 5$

الإثبات :

(أ) إذا كان $n = 1$ ، فإن $2^1 = 2 > 1$ وعليه فإن العبارة أعلاه صحيحة عندما $n = 1$. والآن لنفرض أن العبارة صحيحة عندما $n = m$. إذاً $2^m > m$ ، لكن $2^{m+1} > 2m$ ، $2m \geq m + 1$. إذاً $2^{m+1} > m + 1$ وعليه فإن العبارة أعلاه صحيحة عندما $n = m + 1$ ، وبالتالي فإن $2^n > n$ لكل $n = N^*$.

(ب) لتكن $P(n) : \forall n \geq 5 , 2^n > 5n$. إذاً عندما $n = 5$ ، نجد أن $2^5 = 32 > 25$ وعليه فإن $p(5)$ عبارة صحيحة ، والآن لنفرض أن $P(m)$ صحيحة . إذاً $2^n > 5m$ لكل $5 \leq m < k$ ، ولإثبات صحة العبارة $P(m + 1)$ ، لاحظ أن

$2^m > 5m \Rightarrow 2^{m+1} > 10m = 5m + 5m > 5m + 5 = 5(m + 1)$ ،وعليه، فإن $P(m + 1)$ عبارة صحيحة . إذاً $2^n > 5n$ لكل $n \geq 5$.

□

مثال (٧) :

أثبت أن $\forall n \geq -1 , 2n^3 - 9n^2 + 13n + 25 > 0$

الإثبات :

لتكن $P(n) : \forall n \geq -1 , 2n^3 - 9n^2 + 13n + 25 > 0$. إذاً عندما $n = 1$ ، نجد أن $2(-1)^3 - 9(-1)^2 + 13(-1) + 25 = 1 > 0$ ، وبالتالي فإن $P(1)$ صحيحة . والآن لنفرض أن $P(m)$ صحيحة . إذاً $2m^3 - 9m^2 + 13m + 25 > 0$, $-1 \leq m < n$.

ولإثبات صحة $P(m+1)$ لاحظ أن

$$2(m+1)^3-9(m+1)^2+13(m+1)+25=(2m^3-9m^2+13m+25)+6(m-1)^2$$

لكن $3m^3-9m^2+13m+25>0$ ، لأن $P(m)$ صحيحة ،

$6(m-1)^2\geq 0$ لكل $m\in N^*$ ، إذاً

$2(m+1)^3-9(m+1)^2+13(m+1)+25>0$ ، وعليه فإن $P(m+1)$

صحيحة وبالتالي فإن $P(n)$ صحيحة لكل $n\geq -1$,

□

مثال (٨) :

إذا كان $r,n\in N$ ، فأثبت أن $\binom{n}{r}=\dfrac{n!}{r!(n-r)!}\in N$ لكل $0\leq r\leq n$

الإثبات :

إذا كانت $n=0,1$ ، فإن $\binom{0}{0}=1\in N$, $\binom{1}{0}=1\in N$, $\binom{1}{1}=1\in N$

وعليه فإن العلاقة أعلاه صحيحة عندما $n=0,1$. والآن لنفرض أن

$\binom{m}{r}\in N$ ، $r\leq m\leq n$. ولكي نثبت أن $\binom{m+1}{r}\in N$ ، $0\leq r\leq (m+1)$

لاحظ أن $\binom{m+1}{0}=1\in N$ ، $\binom{m+1}{m+1}=1\in N$ ، كما أن

$$\binom{m+1}{r}=\binom{m}{r}+\binom{m}{r-1} \quad \text{لكل } 1\leq r\leq m \qquad \ldots(1)$$

تسمى العلاقة (1) قاعدة باسكال والتي يجب أن تسمى قاعدة الكرخي أنظر [٣]

لكن $\binom{m}{r}\in N$ ، $\binom{m}{r-1}\in N$ حسب فرضية الأستنتاج الرياضي . إذاً

$\binom{m+1}{r}\in N$ لكل $1\leq r\leq m+1$ ، وعليه فإن $\binom{n}{r}\in N$ لكل $0\leq r\leq n$

□

تمـــــارين

(١) أثبت أن

(أ) $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ لكل $n \in N^*$.

(ب) $\sum_{i=1}^{n} (2i-1) = n^2$ لكل $n \in N^*$.

(ج) $\sum_{i=1}^{n} (4i+1) = 2n^2 + 3n + 1$ لكل $n \in N^*$.

(د) $\sum_{i=1}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2$ لكل $n \in N^*$.

(هـ) إذا كان $a \neq 1$ ، فإن $\sum_{i=1}^{n} a^i = \frac{1-a^{n+1}}{1-a}$.

(و) $\sum_{i=1}^{n} i^4 = \frac{n(n+1)(6n^3+9n^2+n-1)}{30}$ لكل $n \in N^*$.

(ز) $\sum_{i=1}^{n} i^5 = \frac{1}{6}n^6 + \frac{1}{2}n^5 + \frac{5}{12}n^4 - \frac{1}{12}n^2$.

(ح) $\sum_{i=1}^{n} (2i-1)^2 = \frac{n(2n-1)(2n+1)}{3}$.

(ط) $\sum_{i=1}^{n} (2i-1)^3 = n^2(2n^2-1)$ لكل $n \in N$.

(ي) $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$ لكل $n \in N$.

(ك) $\sum_{i=1}^{n} \frac{1}{(2i-1)(2i+1)} = \frac{n}{2n+1}$ لكل $n \in N^*$.

(٢) أثبت أن

(أ) $\sum_{r=1}^{n} r(r!) = (n+1)! - 1$

(ب) $\sum_{r=1}^{n} (r^2+1)\, r! = n(n+1)!$

(ج) $\sum_{r=1}^{n}\frac{r}{(r+1)!}=1-\frac{1}{(n+1)!}$ (د) $\prod_{r=1}^{n}\cos(\frac{x}{2^r})=\frac{\sin x}{2^n\sin(\frac{x}{2^n})}$

(هـ) $n^2<2^n<n!$ لكل $n\geq 5$ (و) $2^n>6n$ لكل $n\geq 5$

(ز) $n!<n^n$ لكل $n\geq 2$

(٣) إذا كان $-1<x\in R$ ، فأثبت أن $(1+x)^n\geq 1+nx$ لكل $n\in N$.

(٤) إذا كان $m\in N$ ، $A\subseteq B=\{\, b\in N \mid b\geq m\}$ بحيث أن $m\in A$ و $(m\in A\Rightarrow n+1\in A)$ ، فأثبت أن $A=B$.

(٥) أثبت أن العبارتين الآتيتين متكافئتان :

(أ) قاعدة الترتيب الجيد (الحسن) . (ب) القاعدة العامة للأستقراء الرياضي.

(٦) " خاصية أرخميدس Archimedean Property "

إذا كان $a,b\in N^*$ ، فبرهن على وجود $n\in N^*$ بحيث أن $na\geq b$.

(٧) إذا كانت $f_1 , f_2 , f_3 , \ldots$ متتابعة فيبوناشي فأثبت أن

(أ) $f_{n+1}\, f_{n+2}-f_n\, f_{n+3}=(-1)^n$ لكل $n\in N^*$.

(ب) $f_n=\frac{a^n-b^n}{\sqrt{5}}$ لكل $n\in N^*$ ، حيث $a=\frac{1+\sqrt{5}}{2}$ ، $a=\frac{1-\sqrt{5}}{2}$.

(ج) $\sum_{i=1}^{n}f_i=f_{n+2}-1$.

(٨) تسمى المتتابعة $1 , 3 , 4 , 7 , 11 , 18 , 29 , \cdots$ متتابعة لوكاس (Lucas sequence) نسبة للرياضي الفرنسي لوكاس (١٨٤٢ – ١٨٩١) والتي تعرّف كالآتي

$L_1=1 \;,\; L_2=3 \;,\; L_{n+2}=L_{n+1}+L_n \;,\; \forall n\in N^*$. أثبت أن

(أ) كلاً من L_{3n-2} ، L_{3n-1} عدد فردي بينما L_{3n} عدد زوجي .

(ب) $L_{n=1}^2 - L_n L_{n+2} = 5(-1)^{n+1}$.

(ج) $L_n = (\frac{1+\sqrt{5}}{2})^n + (\frac{1-\sqrt{5}}{2})^n$ لكل $n \in N^*$.

(٩) أثبت أن

(أ) $\prod_{i=2}^{n} (1-\frac{1}{i^2}) = \frac{n+1}{2n}$ لكل $n \geq 2$.

(ب) $x^n - y^n$ يقبل القسمة على $(x-y)$ لجميع قيم n الزوجية .

(ج) $\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$.

(د) $\prod_{i=1}^{n} a_i \cdot b_i = \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{n} b_i$.

(١٠) إذا كان $a_i \ , b_i \in N^*$ ، فأثبت أن

(أ) $\prod_{i=1}^{n}(a_i + b_i) \geq \prod_{i=1}^{n} a_i + \prod_{i=1}^{n} b_i$

(ب) $\sum_{i=1}^{n} a_i b_i \leq \sum_{i=1}^{n} a_i \cdot \sum_{i=1}^{n} b_i$

****

الفصل الثاني

قابلية القسمة (Divisibility)

يضم هذا الفصل ثلاثة بنود ندرس فيها القسمة الخوارزمية والقاسم المشترك الأعظم ، الأعداد الأولية والمبرهنة الأساسية في الحساب وبعض تطبيقاتها .

٢-١ : القسمة الخوارزمية والقاسم المشترك الأعظم

القسمة هي إيجاد عدد نسبته إلى الواحد كنسبة المقسوم إلى المقسوم عليه ، أما القاسم المشترك الأعظم لعددين أو كثر فهو أكبر العوامل المشتركة بينهما ، ومن الطبيعي وجود خواص لكل منهما وهذا ما نرغب بدراسته في هذا الجزء .

تعريف ٢-١-١ :

إذا كان $a,b\in Z$ ، $b\neq 0$ ، فيقال عن a أنه يقبل القسمة (divisible) على b أو أن b تقسم (divides) a إذا وجد $m\in Z$ بحيث أن $a=bm$.

إذا كان a يقبل القسمة على b فيعبر عن ذلك بالشكل $b\backslash a$ أو $\frac{a}{b}$ ،

أما إذا كان a يقبل القسمة على b فيعبر عن ذلك بالشكل $b\nmid a$.

مثال (١) :

(أ) $3\backslash 6$ ، لأن $6=2\times 3$ بينما $4\nmid 6$ لعدم وجود $m\in Z$ بحيث أن $6=4m$.

(ب) $a\backslash 0$ لكل $m\in Z^*$ ، (ج) $\mp a\backslash a$ لكل $m\in Z^*$

(د) $\mp 1\backslash a$ لكل $m\in Z$

(هـ) إذا كان $a_n=2^{2n-1}+3^{2n-1}$ ، فإن $5\backslash a_n$ لكل $n\in N^*$ ويمكن أثبات ذلك بالاستقراء (الاستنتاج) الرياضي ، لأنه إذا كان $n=1$ ، فإن $a_1=5$ يقبل القسمة على 5 . إذا فرضنا أن $5\backslash a_m$ فإن

$k = \frac{2^{2m-1}+3^{2m-1}}{5} = \frac{a_m}{5}$ ، وعليـــه فـــإن $2^{2m} = 10k - 2\times 3^{2m-1}$

ولكي نثبت أن $5 \backslash a_{m+1}$ ، لاحظ أن

$$\frac{a_{m+1}}{5} = \frac{2^{2m+1}+3^{2m+1}}{5} = \frac{2(10k-2\times 3^{2m-1})+3^{2m+1}}{5} = 4k+3^{2m-1}$$

وعليه فإن $5 \backslash a_{m+1}$. إذاً $5 \backslash a_n$ لكل $m \in N^*$.

والآن إلى بعض خواص القسمة

<u>مبرهنة ٢-١-١ :</u>

إذا كان $a, b, c \in Z$ ، فإن

(أ) $a \backslash \mp 1 \Leftrightarrow a = \mp 1$ (ب) $(b \backslash a \wedge c \backslash b) \Rightarrow c \backslash a$

(ج) $(b \backslash a) \wedge (a \backslash b) \Leftrightarrow a = \mp b$ (د) $(b \backslash a) \wedge c \neq 0 \Rightarrow bc \backslash ac$

(هـ) $c \backslash a \wedge c \backslash b \Rightarrow c \backslash ax + by \quad \forall x, y \in Z$

<u>البرهان :</u>

سنثبت (أ) ، (ج) ، (هـ) ونترك الباقي للقارئ .

(أ) نفرض أن $a \backslash \mp 1$. إذاً يوجد $b \in Z$ بحيث أن $ab = \mp 1$ ، وعليـــه فـــإن $|ab| = |a|\,|b| = 1$. لكن كلاً من a ، b لا يساوي صـــفراً . إذاً $|a| \geq 1$ و $|b| \geq 1$ فإذا كانت $|a| > 1$ أو $|b| > 1$ ، فإن $|ab| > 1$. إذاً $|a| = |b| = 1$ ومنه ينتج أن $a = \mp 1$ ، $b = \mp 1$.

وإذا كان $a = \mp 1$ فمن الواضح أن $a \backslash \mp 1$.

(ج) إذا كان $a = \mp b$ فمن الواضح أن $b \backslash a$ و $a \backslash b$. ولإثبات العكس نفرض أن $b \backslash a$ و $a \backslash b$. إذاً $a = mb$ ، $b = na$ حيث $m, n \in Z$ ، وعليه فإن $a = mna$ ومنه ينتج أن $mn = 1$. إذاً $m = n = \mp 1$ حسب (أ)، وعليـــه فإن $a = \mp b$.

(هـ) بما أن $c \backslash a$ و $c \backslash b$ بالفرض، إذاً $a = mc$ ، $b = nc$ حيث $m,n \in Z$ ، وعليه فإن $ax = mc\,x = (mx)c$ لكل $x \in Z$ و $by = (nc)y = (ny)$ لكل $y \in Z$. إذاً $ax + by = (mx + ny)c$ لكن $mx + ny \in Z$. إذاً $c \backslash ax + by$.

□

مبرهنة ٢-١-٢ : " القسمة الخوارزمية Division Algorithm "

إذا كان $a, b \in Z$ ، $b \neq 0$ فيوجد عددين صحيحين وحيدين m,r بحيث أن $a = mb + r$ ، $0 \leq r < |b|$.

البرهان :

(١) لتكن $b > 0$. إذاً

(أ) إذا كان $0 \leq a < |b|$ ، فإن $a = 0 \cdot b + a$.

(ب) إذا كان $a \geq b > 0$ ، فافرض أن $S = \{ a - xb | x \in Z \ , \ a - xb \geq 0 \}$ إذاً $b \geq 1$ حسب مبرهنة (١-٢-١) ، كما أن $|a|\, b \geq |a|$ ، وعليه فإن $a - (-|a|)b = a + |a|b \geq 0$ ، ومنه ينتج أن $a - xb \in S$ عندما $x = -|a|$ ، وعليه فإن $S \neq \emptyset$. لكن S مجموعة جزئية من N و N مرتبة جيداً حسب قاعدة الترتيب الجيد . إذاً S تحوي عنصر أول (أصغر) وليكن r. إذاً يوجد $m \in Z$ بحيث أن $r = a - mb$ ، وعليه فإن $a = mb + r$ ، $r \geq 0$. ولكي نثبت أن $r < b$ نفرض أن $r \geq b$. إذاً

$a - (m + 1)b = (a - mb) - b = r - b \geq 0$ ، وعليه فإن $r - b \in S$.

لكن $r - b < r$ يناقض كون r عنصر أصغر في S . إذاً $r < b$ ، وعليه فإن $a = mb + r$ ، $0 \leq r < |b|$.

(ج) إذا كان $a < 0$ فإن $-a > 0$ وعليه يوجد $n, t \in Z$ بحيث أن $-a = nb + t$ حيث $0 \leq t < b$ حسب (ب) . إذاً $a = (-n)b - t$ ،

$-b < -t \leq 0$. فإذا كان $t = 0$ فإن $a = -nb$ ، $b > 0$ أما إذا كان $t > 0$ فإن $a = (-n-1)b + (b-t)$ وعليه فإن $a = mb + r$ حيث $m = -n - 1 \in Z$ ، $0 < r = b - t < b$.

(٢) إذا كان $b < 0$ فإن $|b| = -b$ ، $-b > 0$ ، وعليه يوجد $n, r \in Z$ بحيث أن $a = n|b| + r = -nb + r$ ، $0 \leq r < |b|$ حسب (ب) . وبوضع $m = -n$ نجد أن $a = mb + r$ حيث $0 \leq r < |b|$.

ولإثبات وحدانية m, r ، لاحظ أنه إذا كان $a = mb + r = m_1 b + r_1$ ، $0 \leq r < |b|$ ، $0 \leq r_1 < |b|$ فإن $r_1 - r = b(m - m_1)$ ، وعليه فإن $|r_1 - r| = |b|\,|m - m_1|$ ولكن $|r_1 - r| < |b|$. إذاً $0 \leq |m - m_1| < 1$ ، وعليه فإن $|m - m_1| = 0$ حسب مبرهنة (١-٢-١) . إذاً $m = m_1$ حسب مبرهنة (١-٢-١ب) ، وعليه فإن $r = r_1$.

□

مثال (٢) :

(أ) إذا كان $a = 57$ ، $b = 5$ ، فإن $a = 11b + 2$ ، $0 < 2 < 5$.

(ب) إذا كان $a = 81$ ، $b = -14$ ، فإن $a = -5b + 11$ ، $0 < 11 < |b|$.

(ج) إذا كان $a = -273$ ، $b = 17$ ، فإن $a = -17b + 16$ ، $0 < 16 < 17$.

(د) إذا كان $a = 24$ ، $b = 6$ ، فإن $a = 4b + 0$.

والآن إلى بعض تطبيقات القسمة الخوارزمية .

مبرهنة ٢-١-٣ :

(أ) إذا كان $a \in Z$ ، فإما $a^2 = 4m$ أو $a^2 = 4m + 1$ ، $m \in Z$.

(ب) إذا كان a عدداً صحيحاً فردياً ، فإن $a = 4m + 1$ أو $a = 4m + 3$ حيث $m \in Z$ ، وأن $a^2 = 8n + 1$ ، $n \in Z$.

(ج) $\frac{n(n+1)(2n+1)}{6} \in Z$ لكل $n \in Z$.

البرهان :

(أ) بقسمة a على 2 ، نجد أن $a = 2n + r$ ، $0 \le r < 2$ ، وعليه فإن $r = 0,1$. فإذا كان $r = 0$ ، فإن $a = 2n$ ، وعليه فإن $a^2 = 4n^2 = 4m$ ، حيث $m = n^2$. أما إذا كان $r = 1$ ، فإن $a = 2n + 1$ وعليه فإن $a = 4(n^2 + n) + 1$ ، وعندما $m = n^2 + n$ ، نجد أن $a^2 = 4m + 1$.

(ب) بما أن $a = 4m + r$ ، $0 \le r < 4$ حسب مبرهنة القسمة الخوارزمية ، إذاً $r = 0,1,2,3$ وعليه فإن $a = 4m$ أو $a = 4m + 1$ ، أو $a = 4m + 2$ أو $a = 4m + 3$. لكن a عدد فردي بالفرض . إذاً $a = 4m + 1$ أو $a = 4m + 3$. فإذا كان $a = 4m + 1$ ، فإن

$a^2 = 16m^2 + 8m + 1 = 8(2m^2 + 1) + 1$ وبوضع $n = 2m^2 + 1$ ، نجد أن $a^2 = 8n + 1$. أما إذا كان $a = 4m + 3$ ، فإن

$a^2 = 8(2m^2 + 3m + 1) + 1$ ، وبوضع $n = 2m^2 + 3m + 1$ نجد أن $a^2 = 8m + 1$.

(ج) بقسمة n على 6 نجد أن $n = 6m + r$ ، $0 \le r < 6$ ، $m \in Z$ ، وعليه فإن $r = 0,1,2,3,4,5$. فإذا كان $r = 0$ ، فإن $n = 6m$ ، وعليه فإن

$$\frac{n(n+1)(2n+1)}{6} = m(6m+1)(12m+3) \in Z$$

وإذا كان $r = 1$ ، فإن $n = 6m + 1$ ، وعليه فإن

$$\frac{n(n+1)(2n+1)}{6} = (6m+1)(3m+1)(4m+1) \in Z$$

أما إذا كان $r = 2$ ، فإن $n = 6m + 2$ ، وعليه فإن

$$\frac{n(n+1)(2n+1)}{6} = (3m+1)(2m+1)(12m+5) \in Z$$

وإذا كان $r = 3$ ، فإن $n = 6m + 3$ ، وعليه فإن

$$\frac{n(n+1)(2n+1)}{6} = (2m+1)(3m+2)(12m+7) \in Z$$

وإذا كان $r = 4$ ، فإن $n = 6m + 4$ ، وعليه فإن

$$\frac{(n+1)(2n+1)}{6} = (3m+2)\,(6m+5)(4m+3) \in Z$$

وإذا كان $r = 5$ ، فإن $n = 6m + 5$ ، وعليه فإن

$$\frac{n(n+1)(2n+1)}{6} = (m+1)\,(6m+5)(12m+11) \in Z$$

إذاً $\frac{n(n+1)(2n+1)}{6} \in Z$ لكل $n \in Z$

□

وقبل تقديم تطبيق آخر للقسمة الخوارزمية ، نورد ما يلي :

تعريف ٢-١-٢ :

لتكن $b \geq 2$ ، $0 < a \in Z$. يقال عن $(a_n a_{n-1} \cdots a_1 a_0)_b$ ، أنه تمثيل للعدد a بالنسبة للأساس b ، ونكتب $a = (a_n a_{n-1} \cdots a_1 a_0)_b$ إذا وجد $n \geq 0$ ، $a = \sum_{i=0}^{n} a_i\, b^i$ حيث $a_i \in \{0, 1, \cdots, b-1\}$ ، $i = 0, 1, \cdots, n$. تسمى a_i أرقام (digits) العدد a ، وإذا كان $b = 2$ ، يسمى التمثيل التمثيل الثنائي (Binary Representation) والذي يستخدم في الحاسبات ويكون $a_i \in \{0, 1\}$.

وإذا كان $b = 3$ يسمى التمثيل التمثيل الثلاثي (Ternary Representation) وتكون $a_i \in \{0, 1, 2\}$.

وإذا كان $b = 8$ يسمى التمثيل التمثيل الثماني (Octal Representation) وتكون $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7\}$.

وإذا كان $b = 10$ يسمى التمثيل التمثيل العشري (Decimal Representation) وتكون $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

وإذا كـــان $b=16$ يـــسمى التمثيـــل : التمثيـــل الـــستة عـــشري (Hexadecimal Representation) والذي يستخدم في علوم الحاسب وتكون $a_i \in \{0,1,2,\cdots,15\}$ ، وتـــستبدل الأعـــداد 10,11,12,13,14,15 بالحروف A,B,C,D,E,F على التوالي .

وإذا كان $b=60$ يسمى التمثيل الستيني الذي استخدمه البابليون وتكـــون $a_i \in \{0,1,2,\cdots,59\}$.

مثال (٣) :

(أ) $47=(101111)_2$ ، لأن $47=1\times2^5+0\times2^2+1\times2^3+1\times2^2+1\times2^2+1$

(ب) $167=(326)_7$ ، لأن $167=3\times7^2+2\times7+6$.

(ج) $1547=(1547)_{10}$ ، لأن $1547=1\times10^3+5\times10^2+4\times10+7$.

والآن إلى المبرهنة الآتية التي تثبت أن أي عدد صحيح أكبر من الواحد يمكن أن يكون أساساً لنظام عددي .

مبرهنة ٢-١-٤ :

إذا كان a عدداً صحيحاً موجباً ، وكان $1<b\in Z$ فـــيمكن التعبيـــر عـــن a بطريقة وحيدة على الشكل $a=a_nb^n+a_{n-1}b^{n-1}+\cdots+a_1b+a_0$ ، حيـــث $a_n>0$ ، $a_i\in\{0,1,\cdots,b-1\}$.

البرهان :

بإستخدام القسمة الخوارزمية m من المرات نجد أن

$$a=r_0b+a_0 \quad ، \quad 0\le a_0<b \qquad \ldots(1)$$

$$r_0=r_1b+a_1 \quad ، \quad 0\le a_1<b \qquad \ldots(2)$$

$$r_1=r_2b+a_2 \quad ، \quad 0\le a_2<b \qquad \ldots(3)$$

....

....

....

$$r_{m-1}=r_mb+a_m \quad ، \quad 0\le a_m<b \qquad \ldots(m)$$

وإذا كان $r_m > 0$ ، فإن $a > r_0 > r_1 > \cdots > r_m$ وهذه المتوالية تناقصية ولا يمكن أن تستمر إلى مالا نهاية . إذاً يوجد n بحيث أن $r_n = 0$ وبالتالي فإن $r_{n-1} = b \cdot 0 + a_n$.

سنثبت أن $a = (a_n a_{n-1} \cdots a_1 a_0)_b$ ، لإثبات ذلك لاحظ أن من (1) ، (2) ينتج أن

$$a = b(r_1 b + a_1) + a_0 = r_1 b^2 + ba_1 + a_0 \qquad \ldots (*)$$

ومن (*) ، (3) نجد أن

$$a = r_2 b^3 + a_2 b^2 + a_1 b + a_0$$

وبنفس الطريقة يمكن أن نثبت أن

$$a = r_n b^{n+1} + a_n b^n + \cdots + a_2 b^2 + a_1 b + a_0$$

لكن $r_n = 0$. إذاً

$$a = a_n b^n + \cdots + a_2 b^2 + a_1 b + a_0 = (a_n a_{n-1} \cdots a_1 a_0) \qquad \ldots (I)$$

ولإثبات وحدانية ذلك التعبير ، نفرض أن

$$0 \le c_i \le b-1 \text{ ، } a = c_m b^m + c_{m-1} b^{m-1} + \cdots + c_1 b + c_0 \qquad \ldots (II)$$

فإذا كان $n \ge m$ ، يمكننا إضافة معاملات صفرية في التعبير (II) ليكون $n = m$ ، ثم نطرح (II) من (I) فنجد أن

$$(a_n - c_n)b^n + (a_{n-1} - c_{n-1})b^{n-1} + \cdots + (a_1 - c_1)b + (a_0 - c_0) = 0 \ldots (III)$$

وإذا فرضنا أن (II) ، (I) مختلفتان ، فإن ذلك يعني وجود i بحيث أن $a_i - c_i \ne 0$ ، وبالتالي فإن

$$(a_n - c_n)b^n + (a_{n-1} - c_{n-1})b^{n-1} + \cdots + (a_{i+1} - c_{i+1})b^{i+1} = (c_i - a_i)b^i$$

ومنها نجد أن $b \backslash (c_i - a_i)$ ، وعليه فإن $b \backslash |a_i - c_i|$ ، وبالتالي فإن

$$|\, a_i - c_i \,| \ge b \qquad \ldots (IV)$$

لكن $0 \le a_i \le b-1$ ، $0 \le c_i \le b-1$ ، إذاً $|\, a_i - c_i \,| < b$ وهذا يناقض (IV) ، وعليه فإن ذلك التعبير وحيد . □

مثال (٤) :

عبر عن العدد 41 بدلالة الأساس $b=2$.

الحل :

بمـــــــــــــــا أن $41=2(20)+1$ ، $20=10(2)+0$ ، $10=5(2)+0$ ، $5=2(2)+1$ ، $2=1(2)+0$ ، $1=0(2)+1$. إذاً

$$41=1\times 2^5+0\times 2^4+1\times 2^3+0\times 2^2+0\times 2+1=(101001)_2$$

مثال (٥) :

عبر عن العدد 21483 بدلالة الأساس $b=8$.

الحل :

بما أن $21483=2685\times 8+3$ ، $2685=335\times 8+5$ ، $335=41\times 8+7$ ، $41=5\times 8+1$ ، $5=0\times 8+5$ ، إذاً

$$21483=5\times 8^4+1\times 8^3+7\times 8^2+5\times 8+3=(51753)_8$$

مثال (٦) :

عبر عن العدد 31827 بدلالة الأساس $b=16$.

الحل :

$31827=1989\times 16+3$ ، $1989=124\times 16+5$ ، $124=7\times 16+12$ ، $7=0\times 16+7$ ، إذاً

$$31827=7\times(16)^3+12\times(16)^2+5\times(16)+3\times(16)^0=(7C53)_{16}$$

والآن إلى تعريف القاسم المشترك الأعظم لعددين صحيحين أو أكثـــر ودراســـة خواصه وإستخدام القسمة الخوارزمية لإيجاده .

تعريف ٢-١-٣ :

(أ) إذا كان واحد على الأقل من العددين الصحيحين a,b لا يـــساوي صـــفراً ، فيقال عن $d\in N^*$ أنه قاسم مشترك أعظم (greatest common divisor) أو عامل مـــشترك أعلـــى (highest common multiple) لهمـــا إذا كـــان (١) $d\setminus a$ و $d\setminus b$.

(٢) إذا كان $c \in N^*$ وكان $c \backslash a$ و $c \backslash b$ ، فإن $c \backslash d$.

إذا كان d قاسماً مشتركاً أعظماً لعددين a,b ، فقد يعبر عن ذلك بالشكل $d = g \cdot c \cdot d(a,b)$ أو $d = h.c.m(a,b)$ أو $d = (a,b)$.

(ب) إذا كانت $a_1, a_2, \cdots, a_n$ أعداداً صحيحة ليست كلها أصفاراً ، فيقال عن $d = (a_1, \cdots a_n) \in N^*$ أنه قاسم مشترك أعظم للأعداد $a_i \in Z^*$ إذا كان

(١) $d \backslash a_i$ لكل $i = 1, \cdots, n$.

(٢) إذا كان $c \in N^*$ وكان $c \backslash a_i$ لكل i ، فإن $c \backslash d$.

مثال (٧) :

(أ) $(12,18) = (-12,18) = (12,-18) = (-12,-18) = 6$

(ب) $(12,14,91) = 7$

والآن إلى المبرهنة الآتية التي تضمن وجود القاسم المشترك الأعظم وتعبر عنه كتركيبة خطية بدلالتهما .

مبرهنة ٢-١-٥ :

(أ) إذا كان واحد على الأقل من العددين $a, b \in Z$ لا يساوي صفراً ، فيوجد لهما قاسم مشترك أعظم وحيد d ، كما يوجد $m, n \in Z$ بحيث أن $d = am + bn$.

(ب) إذا كان كل من a,b عدد صحيح غير صفري ، وكان $a = bm + r$ ، $0 \le r \le m$ ، فإن $(a,b) = (b,r)$.

البرهان :

(أ) لتكن $S = \{ax + by | x, y \in Z\}$. إذاً إذا كان $b = 0$ فإن $0 < ax + by = |a| \in S$ عندما $x = 1$ ، $a > 0$ أو $x = -1$ ، $a < 0$.
وإذا كان $a = 0$ فإن $0 < ax + by = |b| \in S$ عندما $y = 1$ ، $b > 0$ أو $y = -1$ ، $b < 0$ ، وإذا كان $a \neq 0$ ، $b \neq 0$ ، فإن $0 < a^2 + b^2 \in S$ عندما $x = a$ ، $y = b$ ، إذاً S مجموعة جزئية غير خالية من N .

وبالتالي فإن S تحوي عنصر أول (أصغر) وليكن d ، إذاً يوجد $m,n\in Z$ بحيث أن $d=am+bn$.

ولكي نثبت أن $d=g.c.d(a,b)$ ، لاحظ أنه باستخدام القسمة الخوارزمية يمكننا إيجاد $r,t\in Z$ بحيث أن $a=dt+r$ ، $0\le r<|b|$. إذاً $r=a-dt$ ، لكن $d=am+bn$. إذاً $r=a(1-mt)+b(-nt)$ ، وعليه فإن $r\in S$ ، $r<d$ وهذا يناقض كون d عنصر أول في S . إذاً $r=0$ ، وعليه فإن $d\backslash a$. وبنفس الطريقة يمكن أن نبرهن على أن $d\backslash b$. إذاً d قاسم مشترك للعددين a،b وإذا كان $c\in Z^+$ ، $c\backslash a$ ، $c\backslash b$ فإن $c\backslash(am+bn)$ حسب مبرهنة (٢-١-١هـ) ، وعليه فإن $c\backslash d$. إذاً d قاسم مشترك أعظم للعددين a,b . ولإثبات وحدانية d، نفرض أن $e\in Z^+$ قاسم مشترك أعظم آخر للعددين a,b . إذاً $d\backslash e$ و $e\backslash d$ وعليه فإن $e=d$.

(ب) نفرض أن $d=(a,b)$. إذاً $d\backslash a$ ، $d\backslash b$ ، وعليه فإن $d\backslash a-mb$ وهذا يعني أن $d\backslash r$ ، وبالتالي فإن d قاسم مشترك لكل من r,b . والآن ليكن $c\in N^*$ و $c\backslash b$ ، $c\backslash r$. إذاً $c\backslash bm+r$ ، وعليه فإن $c\backslash a$ ، وبالتالي فإن c قاسم مشترك للعددين a,b . إذاً $c\backslash d$ ، وعليه فإن $d=(b,r)$.

□

نتيجة : إذا كان $a,b,c\in Z$ ، $c>0$ ، فإن $(ac,bc)=c(a,b)$.

البرهان :

ليكن $d=(a,b)$. إذاً يوجد $m,n\in Z$ بحيث أن $d=am+bn$ حسب مبرهنة (٢-١-٥) . لكن $d\backslash a$ و $d\backslash b$ ، إذاً $dc\backslash ac$ ، $dc\backslash bc$ ، وعليه فإن dc قاسم مشترك للعددين ac,bc . والآن لنفرض أن $e\backslash ac$ ، $e\backslash bc$. إذاً $e\backslash acx+bcy$ لكل $x,y\in Z$ حسب مبرهنة (٢-١-١هـ) ، وعليه فإن $e\backslash acm+bcn$ وهذا يعني أن $e\backslash(am+bn)c$ ، وعليه فإن $e\backslash dc$. إذاً $(ac,bc)=dc=c(a,b)$.

ملاحظة :

إذا كان $d=(a,b)=am+bn$ ، فإن m,n ليسا وحيدتين كما يوضح ذلك المثال الآتي .

ليكن $a=18$ ، $b=27$. إذاً

$$9=(18,27)=(-1)(18)+27=2(18)+27(-1)$$

وعلى الرغم من كون مبرهنة (٢-١-٥) تضمن وجود القاسم المشترك الأعظم لأي عددين صحيحين غير صفريين ، فإنها لا تعطي طريقة لإيجاده ، لذا سنورد المبرهنة الآتية (الطريقة الخوارزمية) التي تضمن وجود القاسم المشترك الأعظم وكيفية إيجاده وإيجاد m,n أيضاً .

مبرهنة ٢-١-٦ :

إذا كان a,b عددين صحيحين غير صفريين واستخدمنا القسمة الخوارزمية المتتالية الآتية :

$$\begin{aligned}
a &= bm_1+r_1 \quad ، \quad 0<r_1<|b| \\
b &= r_1m_2+r_2 \quad ، \quad 0<r_1<r_1 \\
r_1 &= r_2m_3+r_3 \quad ، \quad 0<r_2<r_1 \\
r_2 &= r_3m_4+r_4 \quad ، \quad 0<r_4<r_3 \\
&\cdots\cdots\cdots\cdots \\
&\cdots\cdots\cdots\cdots \\
r_{i-2} &= r_{i-1}m_i+r_i \quad ، \quad 0<r_i<r_{i-1} \\
r_{i-1} &= r_im_{i+1}+0
\end{aligned}$$

فإن $r_i=g.c.d(a,b)$. كما أنه يمكن استخدام نفس المعادلات إبتداءً من الأخيرة إلى الأولى لإيجاد $m,n\in Z$ بحيث $r_i=am+bn$.

البرهان :

بما أن $\ldots>r_2>r_1>|b|$. إذاً عدد البواقي لا يمكن أن يزيد عن $(|m|-1)$ ، وعليه يوجد $i\in N$ بحيث أن $r_{i+1}=0$. ولكي نثبت أن $r_i=g.c.d(a,b)$.

لاحظ أن $r_{i-1} = r_i m_{i+1}$ يعني أن $r_i \backslash r_{i-1}$. لكن $r_{i-2} = r_{i-1} m_i + r_i$. إذاً $r_i \backslash r_{i-2}$. وحيث أن $r_{i-3} = r_{i-2} m_{i-1} + r_{i-1}$. إذاً $r_i \backslash r_{i-3}$ ، وعليه يمكن الإستمرار بنفس الأسلوب لنثبت أن $r_i \backslash a$ و $r_i \backslash b$. إذاً r_i قاسم مشترك للعددين a,b . وإذا كان $c \in Z^+$ و $c \backslash a$ ، $c \backslash b$ فمن المعادلة $a = bm_1 + r_1$ نجد أن $c \backslash r_1$. ومن المعادلة $b = r_1 m_2 + r_2$ نجد أن $c \backslash r_2$ وهكذا يمكن استخدام جميع المعادلات الواحدة بعد الأخرى ونصل إلى أن $c \backslash r_i$. إذاً $r_i = g.c.d(a,b)$.

ولإيجاد $m,n \in Z$ بحيث أن $r_i = am + bn$ استخدم المعادلات الواردة في المبرهنة من الأسفل إلى الأعلى تجد أن

$$r_i = r_{i-2} - r_{i-1} m_i = r_{i-2} - (r_{i-3} - r_{i-2} m_{i-1}') m_i$$
$$= -r_{i-3} m_i + r_{i-2}(1 + m_{i-1} m_i) = \cdots = am + bn$$

□

مثال (٨) :

(أ) أوجد القاسم المشترك الأعظم للعددين 252 , 90 ثم أوجد $m,n \in Z$ بحيث أن $d = 252m + 90n$.

لإيجاد d لاحظ أن $252 = 2(90) + 72$ ، $90 = 1(72) + 18$ ، $72 = 4(18)$. إذاً $d = 18$. ولإيجاد $m,n \in Z$ بحيث أن $d = 252m + 90n$. لاحظ أن $72 = 90 - d$. إذاً $252 = 2(90) + 90 - d \Rightarrow d = 252(-1) + 90(3)$. وعليه فإن $m = -1$ ، $n = 3$.

(ب) أوجد القاسم المشترك الأعظم للعددين 2746 ، 335 ثم عبر عنه بالشكل $2746m + 335n$.

لإيجاد القاسم المشترك الأعظم لاحظ أن

$2746 = 8(335) + 66$ ، $335 = 5(66) + 5$ ، $66 = 13(5) + 1$ ، $5 = 5 \times 1$

إذاً $d=1$. ولإيجاد m,n لاحظ أن

$$1=66-5(13)=66-13[335-5(66)]=-13\times335+66\times66$$
$$=-13\times335+66(2746-8\times335)=2746\times66+335(-541)$$

إذاً $m=66$ ، $n=-541$.

ملاحظة :

يمكن حساب القاسم المشترك الأعظم d للعددين a,b وإيجاد $m,n\in Z$ بحيث أن $d=am+bn$ باستخدام طريقة بلانكنشب (Blankinship) . American Mathematical Monthly (1963) وهي :

نفرض أن $a>b>0$ ، وأن $A=\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$ ونضيف (بالتعاقب) مضاعفات أحد الصفوف إلى الصف الآخر "يسمى مثل تلك العمليات –عمليات صفوف أوليه αr_i+r_j " إلى أن نصل إلى مصفوفة بالشكل

$\begin{pmatrix} 0 & x & y \\ d & m & n \end{pmatrix}$ أو $\begin{pmatrix} d & m & n \\ 0 & x & y \end{pmatrix}$ فيكون $d=(a,b)=am+bn$

ونوضح هذه الطريقة بالأمثلة الآتية :

مثال (٩) :

أوجد $d=(a,b)$ ثم أوجد $m,n\in Z$ بحيث أن $d=am+bn$ عندما (أ) $a=39\ ,\ b=18$ ، (ب) $a=1976\ ,\ b=365$.

الحل :

(أ) بما أن $A=\begin{pmatrix} 39 & 1 & 0 \\ 18 & 0 & 1 \end{pmatrix}$ ، وبما أن $39=2(18)+3$ إذاً نضرب الصف الثاني r_2 في (-2) ونجمعه مع الصف الأول r_1 فنجد أن

$$A=\begin{pmatrix} 39 & 1 & 0 \\ 18 & 0 & 1 \end{pmatrix}\xrightarrow{-2r_2+r_1}\begin{pmatrix} 3 & 1 & -2 \\ 18 & 0 & 1 \end{pmatrix}$$

لكن $6(3)=18$. إذاً نضرب الصف الأول في (-6) ونجمعه مع الصف الثاني فنجد أن

$$\begin{pmatrix} 3 & 1 & -2 \\ 18 & 0 & 1 \end{pmatrix} \xrightarrow{-6r_1+r_2} \begin{pmatrix} 3 & 1 & -2 \\ 0 & -6 & 13 \end{pmatrix}$$

إذاً $d=3=39(1)+18(-2)$.

(ب) $A=\begin{pmatrix} 1976 & 1 & 0 \\ 365 & 0 & 1 \end{pmatrix}$ ، $1976=365(5)+151$. إذاً

$A \xrightarrow{-5r_2+r_1} \begin{pmatrix} 151 & 1 & -5 \\ 365 & 0 & 1 \end{pmatrix}$. لكن $365=2(151)+63$ ، إذاً

$$\begin{pmatrix} 151 & 1 & -5 \\ 365 & 0 & 1 \end{pmatrix} \xrightarrow{-2r_1+r_2} \begin{pmatrix} 151 & 1 & -5 \\ 63 & -2 & 11 \end{pmatrix}$$

وحيث أن $151=2(63)+25$، إذاً

$$\begin{pmatrix} 151 & 1 & -5 \\ 63 & -2 & 11 \end{pmatrix} \xrightarrow{-2r_2+r_1} \begin{pmatrix} 25 & 5 & -27 \\ 63 & -2 & 11 \end{pmatrix}$$

وبما أن $63=2(25)+13$. إذاً

$$\begin{pmatrix} 25 & 5 & -27 \\ 63 & -2 & 11 \end{pmatrix} \xrightarrow{-2r_1+r_2} \begin{pmatrix} 25 & 5 & -27 \\ 13 & -12 & 65 \end{pmatrix}$$

وحيث أن $25=13(1)+12$. إذاً

$$\begin{pmatrix} 25 & 5 & -27 \\ 13 & -12 & 65 \end{pmatrix} \xrightarrow{-r_2+r_1} \begin{pmatrix} 12 & 17 & -92 \\ 13 & -12 & 65 \end{pmatrix}$$

لكن $13=12(1)+1$. إذاً

$$\begin{pmatrix} 12 & 17 & -92 \\ 13 & -12 & 65 \end{pmatrix} \xrightarrow{-r_1+r_2} \begin{pmatrix} 12 & 17 & -92 \\ 1 & -29 & 157 \end{pmatrix}$$

وحيث أن $12=12.1$. إذاً

$$\begin{pmatrix} 12 & 17 & -92 \\ 1 & -29 & 157 \end{pmatrix} \xrightarrow{-r_2+r_1} \begin{pmatrix} 0 & 46 & -249 \\ 1 & -29 & 157 \end{pmatrix}$$

وعليه فإن $d=(1976,365)=1=1976(-29)+365(157)$.

والآن إلى المبرهنة الآتية التي توضح كيفية إيجاد القاسم المشترك الأعظم لأكثر من عددين صحيحين .

مبرهنة ٢-١-٧ :

إذا كان $a_1, a_2, \cdots, a_n$ أعداد صحيحة غير صفرية ، $n \geq 3$ فإن :

(أ) ، $d = g.c.d(a_1, \cdots, a_n) = g.c.d(g.c.d(a_1, \ldots, a_n), a_n)$.

(ب) يوجد $r_i \in Z$ بحيث أن $d = \sum_{i=1}^{n} a_i r_i$.

البرهان :

(أ) نفرض أن $d = g.c.d(a_1, \cdots, a_n)$ ، $c = g.c.d(a_1, \cdots, a_{n-1})$ ، $e = g.c.d(c, a_n)$. إذاً $d \backslash a_i$ لكل $i = 1, \cdots, n$ ، وعليه فإن $d \backslash c$ ومنه ينتج أن $d \backslash e$. وحيث أن $e \backslash c$ ، $e \backslash a_n$. إذاً $e \backslash a_i$ لكل $i = 1, \cdots, n$ ، وعليه فإن $e \backslash d$. لكن $e, d \in Z^+$. إذاً $e = d$.

(ب) أستخدم الأستقراء الرياضي على $n \geq 3$ والمبرهنة (٢-١-٥) تحصل على المطلوب .

□

مثال (١٠) :

أوجد القاسم المشترك الأعظم d للأعداد 30,21,66 ثم أوجد $m, n, r \in Z$ بحيث أن $d = 30m + 21n + 66r$.

الحل :

بما أن $d = (30, 21, 66) = ((30, 21), 66)$ ، $g = (30, 21) = 3$. إذاً $d = (3, 66) = 3 = (-21)3 + (1)(66)$. لكن $g = -2(30) + 3(21)$. إذاً $d = (-21)[(-2)(30) + 3(21)] + 66(1) = 42(30) + (-66)(21) + 66(1)$.

مثال (١١) :

أوجد $d = (570, 810, 465, 175)$ ثم أوجد m, n, r, s بحيث أن $d = 570m + 810n + 495r + 175s$.

الحل :

بالقسمة الخوارزمية نوجد $d_1 = (570,810)$ ، فنجد أن

$810 = 1(570) + 240$ ، $570 = 2(240) + 90$ ، $240 = 2(90) + 60$ ،

$90 = 1(60) + 30$ ، $60 = 2(30)$. إذاً

$$\begin{aligned} d_1 &= 30 = 90 - 60 = 90 - [240 - 2(90)] = 3(90) - 240 \\ &= 3[570 - 2(240)] - 240 = 3(570) - 7(240) \\ &= 3(570) - 7(810 - 570) = 10(570) + (-7)(810) \end{aligned}$$

والآن نحسب $d_2 = (d_1, 495) = (30 , 495)$، فنجد أن $495 = 16(30) + 15$ ،

$30 = 2(15)$ ، وعليه فإن

$$\begin{aligned} d_2 &= 15 = 495 - 16d_1 = 495 - 16[10(570) + (-7)(810)] \\ &= 495 + (-160)(570) + 112(810) \end{aligned}$$

لكن $d = (d_2, 175)$ ، إذاً

$$\begin{aligned} d &= (15,175) = 5 = 12(15) + (-1)(175) = 12d_2 + (-1)(175) \\ &= 12[495 + (-160)(570) + 112(810)] + (-1)(175) \\ &= 570(-1920) + 1344(810) + 12(495) + (-1)(175) \end{aligned}$$

□

ولدارسة خواص أخرى للقاسم المشترك الأعظم نورد ما يلي :

تعريف ٢-١-٤ :

يقال عن عددين صحيحين غير صفريين أنهما أوليان نسبياً (relatively prime) إذا كان قاسمهما المشترك الأعظم يساوي واحد .

مثال (١٢) :

(أ) 5,2 أوليان نسبياً ، لأن $1 = (2,5)$.

(ب) 6,11 أوليان نسبياً ، لأن $1 = (11,6)$.

(ج) 8,15 أوليان نسبياً ، لأن $1 = (8,15)$.

(د) 335,2746 أوليان نسبياً ، لأن $1 = (335,2746)$ كما أثبتنا في مثال ٨ب .

مبرهنة ٢-١-٨ :

إذا كان $a,b \in Z^*$ فإن a,b أوليان نسبياً إذاً وإذا فقط وجد $m,n \in Z$ بحيث أن $am+bn=1$.

البرهان :

نفرض أن a,b أوليان نسبياً . إذاً $(a,b)=1$ ، وعليه يوجد $m,n \in Z$ بحيث أن $am+bn=1$ حسب مبرهنة (٢-١-٥) .

ولإثبات العكس نفرض وجود $m,n \in Z$ بحيث أن $am+bn=1$ ولنفرض $d=(a,b)$. إذاً $d \backslash a$ و $d \backslash b$. لكن $d \backslash am+bn$ حسب مبرهنة (٢-١-١هـ) . إذاً $d \backslash 1$ ، لكن $d \in N^*$. إذاً $d=1$ ، وعليه فإن a,b أوليان نسبياً .

□

نتيجة (١) :

إذا كان $a,b \in Z$ و $d=(a,b)$ ، فإن $(\frac{a}{d},\frac{b}{d})=1$

البرهان :

بما أن $d=(a,b)$. إذاً يوجد $m,n \in Z$ بحيث أن $d=am+bn$ حسب مبرهنة (٢-١-٥) ، وعليه فإن $1=\frac{a}{d}m+\frac{b}{d}n$ ، وبالتالي فإن $(\frac{a}{d},\frac{b}{d})=1$ حسب مبرهنة (٢-١-٨) .

□

نتيجة (٢) :

إذا كان $a,b,c \in Z$ وكان $b \backslash a$ ، $c \backslash a$ ، و $(b,c)=1$ ، فإن $bc \backslash a$.

البرهان :

بما أن $b \backslash a$ و $c \backslash a$. إذاً يوجد $r,s \in Z$ بحيث أن $a=br=cs$. لكن $(b,c)=1$. إذاً يوجد $m,n \in Z$ بحيث أن $bm+cn=1$ حسب مبرهنة (٢-١-٥) ، عليه فإن $a=a\,bm+a\,cn=bcsm+bcrn=bc(sm+rn)$ ، وبالتالي فإن $bc \backslash a$.

مبرهنة ٢-١-٩ : لتكن $a,b,c \in Z$.

(أ) إذا كان $(a,b)=1$ و $(a,c)=1$ ، فإن $(a,bc)=1$.

(ب) إذا كان $c \backslash ab$ ، وكان $(b,c)=1$ فإن $c \backslash a$.

البرهان :

(أ) بما أن $(a,b)=1$ ، $(a,c)=1$ بالفرض . إذاً يوجد $m,n \in Z$ بحيث أن $am+bn=1$ ، ويوجد $r,s \in Z$ بحيث أن $ar+cs=1$ حسب مبرهنة (٢-١-٥أ) ، وعليه فإن $am+bn(ar+cs)=1$ ، ومنه ينتج أن $a(m+bnr)+bc(ns)=1$ ، وعليه فإن $(a,bc)=1$ حسب مبرهنة (٢-١-٨)

(ب) بما أن $(b,c)=1$ بالفرض . إذاً يوجد $m,n \in Z$ بحيث أن $bm+cn=1$ حسب مبرهنة (٢-١-٥أ) ، وعليه فإن $a\,bm+a\,cn=a$. لكن $c \backslash ab$ بالفرض و $c \backslash ac$. إذاً $c \backslash a\,bm+a\,cn$ حسب مبرهنة (٢-١-١هـ) ، وعليه فإن $c \backslash a$.

تمارين

(١) إذا كان $n \in N^*$ ، فأثبت أن :

(أ) 5^n-2^n يقبل القسمة على 3 .

(ب) (7^n-5^n) عدد زوجي .

(ج) $3^{2n-1}+4^{2n-1}$ يقبل القسمة على 7 .

(د) $2^{2n}-1$ يقبل القسمة على 3 .

(هـ) $(5^{2n}-1)$ يقبل القسمة على 24 .

(و) $2^{3n}-1$ يقبل القسمة على 7.

(ز) $3^{2n}+7$ يقبل القسمة على 8 .

(ح) $2^n+(-1)^{n+1}$ يقبل القسمة على 3 .

(ط) $10^{n+1}-9n-10$ يقبل القسمة على 81 .

(٢) أثبت بإستخدام القسمة الخوارزمية أن :

(أ) كل عدد صحيح فردي يكون على الشكل $4m+1$، $4m+3$ ، $m \in Z$.

(ب) يمكن التعبير عن مربع أي عدد صحيح بالشكل $3m$ أو $3m+1$ ، $m \in Z$.

(ج) يمكن التعبير عن مكعب أي عدد صحيح بالشكل $9m$ أو $9m+1$ أو $9m+8$ ، $m \in Z$.

(٣) أثبت أن $a_n \in Z \; , \; \forall n \in Z$ عندما :

(أ) $a_n = \dfrac{n(n+1)}{2}$ ، (ب) $a_n = \dfrac{n(n+1)(n+2)}{3}$.

(ج) $a_n = \dfrac{n^3+5n}{6}$.

(٤) إذا كان n عدداً فردياً ، فأثبت أن n^2-1 يقبل القسمة على 8 .

(٥) أثبت أن أي عدد في حدود المتتابعة $11 , 111 , 1111 , \cdots$ لا يمكن أن يكون مربعاً كلاماً . " لاحظ أن أي حد من حدود المتتابعة يمكن كتابته بالشكل $4m+3$ "

(٦) إذا كان a, b عددين صحيحين فرديين فأثبت a^2+b^2 عدد زوجي لا يقبل القسمة على 4 .

(٧) عبر عن كل من الأعداد 179 ، 527 ، 13429 ، 31535 بدلالة الأساس $b=2$ ، $b=7$ ، $b=8$ ، $b=12$ ، $b=16$.

(٨) لتكن $a,b,c \in Z$ ، $(a,b)=1$. فأثبت أن .

(أ) إذا كان $c \backslash a$ ، فإن $(b,c)=1$.

(ب) $(ac,b)=(c,b)$.

(ج) $(a+b\,,\,a-b)=1$ أو $(a+b\,,\,a-b)=2$.

" ملاحظة : أفرض أن $d=(a+b\,,\,a-b)$ ثم أثبت أن $d \backslash 2a$ و $d \backslash 2b$ وبالتالي فإن $d \le (2a\,,\,2b))=2$ ".

(د) $(a^n, b^n) = 1$ ، $n \in N^*$.

(هـ) إذا كان $c \backslash (a+b)$ ، فإن $(a,c) = (b,c) = 1$.

(٩) (أ) إذا كان $(a, bc) = 1$ ، فأثبت أن $(a,b) = 1 \;,\; (a,c) = 1$.

(ب) إذا كان $c \neq 0$ ، فأثبت أن $(ac, bc) = |c|(a,b)$.

(ج) إذا كان $b \backslash c$ ، فأثبت أن $(a,b) = (a+c, b)$.

(د) إذا كان $(b,c) = 1$ ، فأثبت أن $(a,bc) = (a,b)(a,c)$.

(هـ) إذا كان $c = am + bn$ ، $m,n \in Z^+$ ، فأثبت أن $(a,b) \backslash c$.

(١٠) أوجد $d = (a,b)$ ، ثم أوجد $m,n \in Z$ بحيث أن $d = am + bn$ عندما :

(أ) $a = 288 \;,\; b = 51$ (ب) $a = 1292 \;,\; b = 884$

(ج) $a = 8633 \;,\; b = 7209$ (د) $a = 7469 \;,\; b = 2387$

(١١) أوجد $d = (a,b,c)$ ، ثم أوجد $m,n,r \in Z$ بحيث أن $d = am + bn + cr$ عندما :

(أ) $a = 33 \;,\; b = 143 \;,\; c = 8749$ (ب) $a = 120 \;,\; b = 60 \;,\; c = 165$

(ج) $a = 1131 \;,\; b = 594 \;,\; c = 2907$.

(١٢) أوجد $d = (a,b,c,e)$ ، ثم أوجد $m,n,r,s \in Z$ بحيث أن $d = am + bn + cr + es$ عندما :

(أ) $a = 116 \;,\; b = 248 \;,\; c = 148 \;,\; e = 152$

(ب) $a = 113 \;,\; b = 594 \;,\; c = 2907 \;,\; e = 1517$

(ج) $a = 21355 \;,\; b = 17801 \;,\; c = 11503 \;,\; e = 8752$

(١٣) يمكن إستخدام الطريقة الآتية للتعبير عن العدد a بدلالة الأساس 2 وهي : ليكن 2^{n_1} أكبر عدد صحيح بحيث أن $2^{n_1} \leq a$ ، وليكن 2^{n_2} أكبر عدد صحيح بحيث أن $2^{n_2} \leq a - 2^{n_1}$ ، وليكن 2^{n_3} أكبر عدد صحيح بحيث أن $2^{n_3} \leq a - 2^{n_1} - 2^{n_2}$. إذاً

$$0 \leq a - (2^{n_1} + 2^{n_2} + 2^{n_3}) < a - (2^{n_1} + 2^{n_2}) < a - 2^{n_1} < a$$

وبنفس الأسلوب يمكن أن نصل إلى الآتي :

$$a-(2^{n_1}+2^{n_2}+\cdots 2^{n_r}) \Rightarrow a=2^{n_1}+2^{n_2}+\cdots 2^{n_r}$$

فمثلاً للتعبير عن العدد 147 بدلالة الأساس 2 ، لاحظ أن $2^7<147$ ، وبالتالي فإن $147-2^7=19$ ، $2^4<19$ ، وعليه فإن $19-16=3$ ، $2<3$ ومنها نجد أن $3-2=1$ و $1=2^0$. إذاً

$$147=2^7+19=2^7+2^4+3=2^7+2^4+2+1$$
$$=2^7+0\times2^6+0\times2^5+1\times2^4+0\times2^3+0\times2^2+1\times2+1$$

وعليه فإن $147=(10010011)_2$.

عبّر بإستخدام هذه الطريقة عن كل من 388، 945 بدلالة الأساس 2 .

□

٢-٢ : الأعداد الأولية Prime Numbers

تكمن أهمية الأعداد الأولية في تطبيقاتها الهندسية من جهة ، وأعتبارها حجر الأساس في بناء الأعداد الصحيحة من جهة أخرى ، وهذا ما نرغب بدراسته في هذا الجزء الذي يضم تعريف العدد الأولي ودراسة خواصه الأساسية

تعريف ٢-٢-١ :

(أ) يقال عن $P\in N^*$ أنه عدد أولي (Prime Number) ، إذا كان $p>1$ ولا يقبل القسمة إلا على P و 1 .

(ب) يقال عن $1<a\in Z$ ، أنه عدد مؤلف (Composite number) ، إذا كان a عدداً غير أولي .

مثال (١) :

(أ) 2,3,5,7,11,13,17,19,23 أعداد أوليه بينما 6 عدد مؤلف لأن 6 يقبل القسمة على 2 .

(ب) 2 + !5 عدد مؤلف ، لأن 2 + !5 يقبل القسمة على 2 . لاحظ أن $5!+2=2(61)$.

(ج) $5!+3$ عدد مؤلف ، لأنه يقبل القسمة على 3 ، كما أن $5!+3=3(41)$ ، $1<3<(5!+3)$ ، $1<41<(5!+3)$.

مبرهنة ٢-٢-١ :

إذا كان $n>2$ ، فإن n عدد مؤلف إذاً وإذا فقط وجد $a,b\in Z$ ، بحيث أن $n=ab$ ، $1<a<n$ ، $1<b<n$

" يسمى كل من a,b عامل من عوامل n "

البرهان :

إذا كان $n=ab$ ، $1<a<n$ ، $1<b<n$ ، فمن الواضح أن n عدد مؤلف . ولإثبات العكس نفرض أن n عدد مؤلف . إذاً يوجد $1\neq a\neq n$ و $a\backslash n$ وعليه يوجد $b\in Z$ بحيث أن $n=ab$ ، لكن $n,a\in Z^+$. إذاً $b\in Z^+$ ، وعليه فإن $1\leq a$ ، $1\leq b$. لكن $a\backslash n$ و $b\backslash n$. إذاً $a\leq n$ و $b\leq n$. لكن $a\neq 1$ ، $a\neq n$. إذاً $1<a<n$. وإذا كان $b=1$ ، فإن $n=a$ وهذا غير ممكن . إذاً $b\neq 1$. وإذا كان $b=n$ ، فإن $a=1$ وهذا غير ممكن . إذاً $1<b<n$.

□

ملاحظة :

كل الأعداد الأولية فردية ما عدا العدد 2 ، وكل منها على الشكل $4m+1$ أو $4m-1$ حيث $m\in Z^+$ ، لأن أي عدد صحيح يمكن كتابته بالشكل

$$4m\ ,\ 4m+1\ ,\ 4m+2\ ,\ 4m+3\quad ، \quad m\in Z$$

لكن $4m$ ليس أولياً ، كما أن $2\backslash 4m+2$ ، وعليه فإن $4m+2$ عدد أولي عندما $m=0$ و 2 عدد أولي زوجي . إذاً أي عدد أولي فردي على الشكل $4m+1$ ، $4m+3$. لكن $S=\{4m+3 \mid m\in n\}=\{4m-1 \mid m\in n^*\}$

إذاً كل عدد أولي فردي على الشكل $4m-1$ أو $4m+1$ ، $m\in n^*$

ولأهمية الأعداد الأولية وضع العلماء تخمينات (Conjectures) كثيرة عليها منها :

(أ) يوجد عدد لا نهائي من الأعداد الأولية على الشكل n^2+1 ، $n \in n^*$
وهذا الحدس أو التخمين لم يثبت بعد . لاحظ أن $2=1^2+1$ ، $5=2^2+1$ ، $17=4^2+1$ ، $37=6^2+1$ ، $197=(14)^2+1$.

(ب) حدس جولدباخ (١٦٩٠-١٧٦٤م) عام ١٧٤٢م :
يمكن التعبير عن أي عدد صحيح زوجي أكبر من 2 كمجموع عددين أوليين .
لاحظ أن $4=2+2$ ، $6=3+3$ ، $8=3+5$ ، $1=3+7$ ، $12=5+7$ ، $14=7+7$ ، $16=5+11$.
وإذا كان حدس جولدباخ صحيحاً ، فإن ذلك يعني أنه يمكن العبير عن أي عدد فردي أكبر في 5 كمجموع ثلاثة أعداد فردية ، لأن إذا كان $n>5$ عدداً فردياً فإن $n-3$ عدد زوجي أكبر من 2 وعليه فإن $n-3=p+q$ ، حيث p,q عددين أوليين وبالتالي فإن $n=p+q+3$.

(ج) يوجد عدد لا نهائي من الأعداد الأولية على الشكل $p, p+2$ ، حيث p عدد أولي . يسمى مثل تلك الأعداد أعداد أولية توأميه (Twin primes) مثل $3,5$ ، $11,13$ ، $17,19$.

(د) تخمين أو حدس الفرنسي لاجرانج (١٧٣٦-١٨١٣) عام ١٧٧٥م : إذا كان n عدداً صحيحاً فردياً أكبر من 5 ، فإن $n=p_1+2p_2$ ، حيث p_1، p_2 عددين أوليين .

والآن إلى التعريف الآتي :

تعريف ٢-٢-٢ :

الترتيب الطبيعي للأعداد الأولية هو $p_1 = 2, p_3 = 5, \cdots, p_n, \cdots$ ويسمى p_n العدد الأولى النوني في الترتيب الطبيعي .

ويمكن أن نبرهن ما يلي .

مبرهنة ٢-٢-٢ :

$p_n \le 2^{2^{m-1}}$ لكل $n \in n^*$.

البرهان : (باالأستقراء على n)

إذا كان $n = 1$ ، فإن $p_1 = 2$ وعليه فإن العلاقة صحيحة عندما $n = 1$.

والآن لنفرض أن العلاقة أعلاه صحيحة عندما $n = m$ ، إذاً $p_m \le 2^{2^{m-1}}$.

ولإثبات صحة العلاقة عندما $n = m + 1$. لاحظ أن

$$p_{m+1} \le p_1 p_2 \cdots p_m + 1 \le 2 \cdot 2^2 \cdots 2^{2^{m-1}} + 1$$

لكن $2 \cdot 2^2 \cdots 2^{2^{m-1}} = 2^{1+2+\cdots 2^{m-1}}$ ، $1 + 2 + \cdots + 2^{m-1} = 2^m - 1$. إذاً $p_{m+1} \le 2^{2^m - 1} + 1$. لكن $1 \le 2^{2^m - 1}$ لكل $m \in N$. إذاً $p_{m+1} \le 2^{2^m - 1} + 2^{2^m - 1} = 2 \cdot 2^{2^{m-1}} = 2^{2^m}$ ، وعليه فإن العلاقة أعلاه صحيحة عندما $n = m + 1$. إذاً $p_n \le 2^{2^{n-1}}$ لكل $m \in N^*$

□

نتيجة :

إذا كان $n \ge 1$ عدداً صحيحاً ، فيوجد على الأقل $n + 1$ من الأعداد الأولية كل منها أقل من 2^{2^n} .

البرهان :

بما أن كلاً من $p_1, p_2, \cdots, p_{n+1}$ أقل من 2^{2n} حسب مبرهنة (٢-٢-٢) . إذاً يوجد على الأقل $(n + 1)$ من الأعداد الأولية كل منها أقل من 2^{2n} .

□

مبرهنة ٢-٢-٣ :

(أ) إذا كان $a,b \in Z$ ، p عدداً أولياً كان $p \backslash ab$ فإما $p \backslash a$ أو $p \backslash b$.

(ب) إذا كان $a_1,\cdots,a_n \in Z$ و p عدداً أولياً وكان $p \backslash a_1a_2\cdots a_n$ فإن $p \backslash a_i$ لبعض قيم $1 \le i \le n$.

البرهان :

(أ) نفرض أن $p \backslash ab$ ، $p \backslash b$. إذاً $(b,p)=1$ ، وعليه فإن $p \backslash a$ حسب مبرهنة (٢-١-٩ب) .

(ب) (بالأستقراء الرياضي على n) .

فإذا كان $n=1$ فإن $p \backslash a_1$ بالفرض ، وعليه فإن النتيجة صحيحة في هذه الحالة . والآن لنفرض أن النتيجة صحيحة عندما $n=m$. ولكي نثبت صحة النتيجة عندما $n=m+1$. لاحظ أنه إذا كان $p \backslash (a_1a_2\cdots a_{m+1})$ فإن $p \backslash a_1(a_2\cdots a_{m+1})$ وعليه إما $p \backslash a_1$ أو $p \backslash (a_2\cdots a_{m+1})$ حسب (أ) فإذا كان $p \backslash a_1$ فقد أنتهى البرهان ، أما إذا كان $p \nmid a_1$ ، فإن $p \backslash a_2\cdots a_{m+1}$ ، وعليه يوجد $2 \le i \le m+1$ بحيث أن $p \backslash a_i$ حسب فرضية الأستقراء الرياضي . إذاً النتيجة صحيحة عندما $n=m+1$. وعليه فإنها صحيحة لجميع قيم $n \in N^*$.

□

مبرهنة ٢-٢-٤ :

(أ) كل عدد صحيح أكبر من الواحد يقبل القسمة على عدد أولي .

(ب) مجموعة الأعداد الأولية لا نهائية .

البرهان :

(أ) نفرض أن

$S=\{n \in Z^+ \mid$ أكبر من الواحد ولا يقبل القسمة على عدد أولي $n\} \neq \phi$.

إذاً S تحوي عنصر أول (أصغر) وليكن m . إذاً m أكبر من الواحد ولا يقبل القسمة على عدد أولي فإذا كان m عدداً أولياً فإن $m\backslash m$ وهذا خلاف الفرض، أما إذا كان m غير أولي ، فإن $r\backslash m$ ، $1\neq r\neq m$ ، وعليه فإن $r<m$ ، ومنه ينتج أن $r\notin S$ ، وبالتالي فإن r يقبل القسمة على عدد أولي وليكن p ، وعليه فإن $p\backslash m$ وهذا خلاف الفرض أيضاً . إذاً $S=\varnothing$.

(ب) نفرض أن مجموعة الأعداد الأولية مجموعة منتهية وأن عنصرها هي $p_1,p_2,\cdots,p_n$. وليكن $n=1+(p_1\dots p_n)$. إذاً $n>1$ ، وعليه فإن n يقبل القسمة على عدد أولى مثل p (حسب أ) . فإذا كان $p=p_i$ لبعض قيم $1\leq i\leq n$ ، فإن $p\backslash n$ و $p\backslash(p_1p_2\cdots p_n)$ ، وعليه فإن $p\backslash 1$، ومنه ينتج أن $p=1$ وهذا يناقض كون p عدداً أولياً . إذاً $p\neq p_i$ لكل $i=1,2,\cdots,n$ ، وعليه فإن مجموعة الأعداد الأولية مجموعة لا نهائية .

□

نتيجة (١) :

لكل عدد مؤلف n قاسم أولي p بحيث أن $p\leq\sqrt{n}$.

البرهان :

بما أن n عدد مؤلف . إذاً $n=ab$ ، $1<a\leq b$ ، وعليه فإن $a^2\leq n$ ، وبالتالي فإن $a\leq\sqrt{n}$. وبتطبيق مبرهنة (٢-٢-٤أ) يمكننا إيجاد عدد أولي p بحيث أن $p\backslash a$. لكن $a\backslash n$. إذاً $p\backslash n$ و $p\leq a$ ، وعليه فإن $p\leq\sqrt{n}$.

□

والآن إلى النتيجة المهمة الآتية والتي يجب أن تنسب إلى ابن طاهر البغدادي (المتوفي سنة ١٠٣٧م ، بدلاً من فيبوناشي (١١٨٠-١٢٥٠م) .

نتيجة (٢) :

إذا لم يكن للعدد $n>1$ قاسماً أولياً أقل من أو يساوي $\sqrt{n}$ ، فإن n عدد أولى .

البرهان :

نفرض أن n عدد غير أولي . إذاً n عدد مؤلف وعليه يوجد عدد أولي p بحيث أن $p \backslash n$ ، $p \le \sqrt{n}$ حسب نتيجة (١) ، وهذا خلاف الفرض .

□

مثال (٢) :

أثبت أن 257 عدد أولى .

الإثبات :

بما أن $17 < \sqrt{257} < 16$ ، إذاً الأعداد الأولية الأقل من أو تساوي $\sqrt{257}$ هي $2,3,5,7,11,13$. لكن $257 = 128(2) + 1$ ، $257 = 85(3) + 2$ ، $257 = 51(5) + 2$ ، $257 = 36(7) + 5$ ، $257 = 23(11) + 4$ ، $257 = 9(13) + 10$. إذاً 257 لا يقبل القسمة على أي من $2,3,5,7,11,13$ وعليه فإن 257 عدد أولى حسب (نتيجة ٢) .

وهذا ولنتيجة (٢) تطبيق آخر إذ بإستخدامها وإستخدام ما يسمى " غربال أيراتوستين Crible d' Eratosthene ، (٢٧٦-١٦٤ ق.م) ، أمين مكتبة الإسكندرية وأول من حسب محيط الأرض بطريقة هندسية " . يمكننا إيجاد الأعداد الأولية الأقل من أو تساوي العدد n .

فإذا كان المطلوب إيجاد الأعداد الأولية الأقل من 90 نكتب جميع الأعداد بين 2 ، 90 ، ثم نشطب مضاعفات الأعداد الأولية التي تقل عن أو تساوي $\sqrt{90}$ وهي مضاعفات الأعداد $2,3,5,7$ فما بقى من تلك الأعداد يكون أعداد أوليه .

إذاً الأعداد الأولية الأقل من $\sqrt{90}$ هي :

$$2,3,5,7,11,13,19,23,29,31,37,41,43,47,53,$$
$$59,61,67,71,73,79,83,89$$

وبإستخدام غربال إيراتوستين ونتيجة (٢) ، نلاحظ أن الأعداد الأولية الواقعة بين 120 ، 180 هي :

$$127,131,137,139,149,151,157,163,167,173,179$$

وحيث أن لكل عدد صحيح موجب n يوجد على الأقل n من الأعداد المؤلفة $(n+1)!+2 , (n+1)!+3 , \cdots , (n+1)!+(n+1)$ لأن $m \backslash (n+1)!+m$ لكل $2 \le m \le n+1$. إذاً توزيع الأعداد الأولية غير منتظم بين الأعداد الصحيحة ، والسؤال الذي يطرح نفسه هو : هل يمكن إحصاء الأعداد الأولية $\pi(x)$ التي تقل عن أو تساوي العدد الحقيقي x ؟ وللإجابة على السؤال : لاحظ أن $\pi(x) = |\{ p \in N : p \le x, \text{ عدد أولي } p\}|$ ، وعليه فإن $\pi(8) = 4$ ، وقد حسب الألماني جاوس (١٧٧٧-١٨٥٠م) $\pi(3\times10^6)$ فوجد أن $\pi(3\times10^6) = 216816$ ، ولاحظ عام (١٧٩١م) أن معدل ازدياد $\pi(x)$ هو نفس معدل ازدياد كل من $\frac{x}{\ln x}$ ، $\mathrm{Lin}(x) = \int_2^x \frac{du}{\ln u}$ وتوقع صحة المبرهنة الآتية والتي تسمى مبرهنة الأعداد الأولية "The prime number theorem" .

مبرهنة ٢-٢-٥ :

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1$$

هذا ولقد خمّن الفرنسي لجندر (١٧٥٢-١٨٣٣م) عام ١٧٩٨ بأن

$$\pi(x) \approx \frac{x}{\ln x - 1.08366}$$

ومن مبرهنة (٢-٢-٥) ، نجد أن $\lim_{x\to\infty} \frac{\pi(x)}{x} = \lim_{x\to\infty} \frac{1}{\ln x} = 0$ ، وعليه فإن لكل a نجد أن

$$\lim_{x\to\infty} \frac{\pi(x)\,(\ln x - a)}{x} = \lim_{x\to\infty} [\frac{\pi(x)\ln x}{x} - \frac{a\,\pi(x)}{x}] = 1$$

وعليه فإن $\pi(x) \approx \frac{x}{\ln x - a}$ لكل a .

أما أول محاولة لإثبات مبرهنة الأعداد الأولية فقط كانت من قبل الروسي شبيشيف (Tchebychef) (١٨٢-١٨٩٤م) ببرهانه على وجود ثابتين a,b ، $a<1<b$ بحيث أن $a\left(\frac{x}{ln x}\right)<\pi(x)<b\left(\frac{x}{ln x}\right)$ عندما x كبيرة كبراً كافياً ، ثم أثبت أنه إذا كان $\lim_{x\to\infty}\frac{\pi(x)ln x}{x}$ موجوداً فإن $\lim_{x\to\infty}\frac{\pi(x)ln x}{x}=1$ ، لكنه لم يتمكن من إثبات وجود تلك النهاية .

هذا وقد أثبت شبيشيف عام ١٨٥٠م بأن

$$\frac{0.89x}{ln x}<\pi(x)<\frac{1.11x}{ln x}$$

وفي عام ١٨٥٩م وسع الألماني ريمان (١٨٢٦-١٨٦٦م) مفهوم دالة زيتا (Zeta function) $\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$ ، $s\in C$ ، والمعرفة من قبل السويسري أويلر (١٧٠٧-١٧٨٣م) بالنسبة للأعداد الحقيقية ، موضحاً العلاقة بين توزيع الأعداد الأولية . وسلوك الدالة $\zeta(s)$ مبيناً العلاقة بين $\pi(x)$ وجذور الدالة $\zeta(s)$ في المستوى s (s-plane) ، ولريمان العديد من التخمينات الخاصة بتوزيع جذور الدالة زيتا أشهرها ما يسمى فرضية ريمان (Riemann Hypothesis) التي تنص على أن جميع الجذور (أصفار) غير الحقيقية للدالة زيتا والتي جزئها الحقيقي موجب تقع على المستقيم $Re(s)=\frac{1}{2}$

هذا وقد خمّن العلماء أن $|\pi(x)-Lin(x)|\le\sqrt{2}ln(x)$ لكل $x\ge 2.01$ ، وفي عام ١٨٩٦م قدم كل من الفرنسي هادمارد (١٨٦٥-١٩٦٣م) والبلجيكي فاليه بواسون (١٨٦٦-١٩٦٢م) أول أثبات لمبرهنة الأعداد الأولية ، ثم تعددت البراهين المعتمدة على الدوال المركبة إلى أن قدم النرويجي سلبرج (١٩١٧-) عام ١٩٤٩م برهاناً لا يعتمد على الدوال المركبة إطلاقاً منح عليه جائزة فيلد في الرياضيات عام ١٩٥٠م .

والآن إلى المبرهنة الآتية :

مبرهنة ٢-٢-٦ :

إذا كان $a>1$ ، $n>1$ عددين صحيحين وكان a^n-1 عدداً أولياً ، فإن $a=2$ و n عدد أولي .

البرهان :

بما أن $a^n-1=(a-1)(a^{n-1}+\cdots+a+1)$. إذاً عندما $a>2$ ، $n>1$ نجد أن $a-1>1$ و $a^{n-1}+\cdots+a+1>a+1>3$ ، وعليه فإن a^n-1 ليس أولياً وهذا خلاف الفرض . إذاً إذا كان a^n-1 أولياً ، فإن $a=2$. والآن لنفرض أن 2^n-1 عدد أولي وأن n ليس أولياً. إذاً $n=rs$ ، $1<r<n$ ، $1<s<n$ حسب مبرهنة (٢-٢-١) ، وعليه فإن $2^n-1=2^{rs}-1=(2^r)^s-1$ عدد أولي . لكننا أثبتنا أعلاه ، أنه إذا كان a^n-1 عدداً أولياً ، فإن $a=2$. إذاً $2^r=2$ ، وعليه فإن $r=1$ ، $s=n$ ، وبالتالي فإن n غير مؤلف . إذاً n عدد أولي .

□

وأخيراً نورد المبرهنة الآتية والتي تعتمد عليها ما يسمى طريقة فيرما (١٦٠١-١٦٦٥م) لتحليل الأعداد الفردية إلى عواملها الأولية .

مبرهنة ٢-٢-٧ :

يمكن التعبير عن أي عدد فردي موجب كحاصل ضرب عدد بين موجبين إذ وإذا فقط أمكن التعبير عنه كفرق بين مربعين .

البرهان :

نفرض أن n عدد فردي موجب ، $n=ab$. إذاً $n=(\frac{a+b}{2})^2-(\frac{a-b}{2})^2$ وكل من a,b عدد فردي . ولإثبات العكس نفرض أن $n=c^2-e^2=(c-e)(c+e)$. إذاً n هو حاصل ضرب عددين موجبين .

ملاحظة :

لتطبيق مبرهنة (٢-٢-٧) نبحث عن حل للمعادلة $a^2 - b^2 = n$ ، وذلك بإيجاد مربع كامل على الصورة $a^2 - n$ ، وعليه يجب البحث عن مربع كامل بين حدود المتتابعة $m^2 - n , (m+1)^2 - n , \cdots$ ، حيث m أصغر عدد صحيح موجب بحيث أن $\sqrt{n} < m$.

مثال (٣) :

حلل العدد 133 إلى عوامله الأولية .

الحل :

بما أن $11 < \sqrt{133} < 12$. إذاً $12^2 - 133 = 11$ ، $13^2 - 133 = 36 = 6^2$، وعليه فإن $133 = 13^2 - 6^2 = (13+6)\,(13-6) = 19 \times 7$ وكل من 7,19 عدد أولي .

مثال (٤) :

حلل العدد 13345 إلى عوامله الأولية .

الحل :

بما أن $115 < \sqrt{13345} < 116$. إذاً

$(116)^2 - 13345 = 13456 - 13345 = 111$ ، و 111 ليست مربعاً كاملاً

$(117)^2 - 13345 = 13689 - 13345 = 344$ ، و 344 ليست مربعاً كاملاً

$(118)^2 - 13345 = 13924 - 13345 = 679$ ، و 679 ليست مربعاً كاملاً

$(119)^2 - 13345 = 14161 - 13345 = 816$ ، و 816 ليست مربعاً كاملاً

$(120)^2 - 13345 = 14400 - 13345 = 1045$ ، و 1045 ليست مربعاً كاملاً

$(121)^2 - 13345 = 14641 - 13345 = 1296 = (36)^2$. إذاً

$$n = 13345 = (121)^2 - (36)^2 = (121+36)(121-36) = 157 \times 85$$

لكن 157 عدد أولي ، لأن $13 > \sqrt{157} > 12$ والأعداد الأولية الأقل من أو تساوي $\sqrt{157}$ هي :

$2,3,5,7,11$ و $157 = 77(2)+1$ ، $157 = (52)(3)+1$ ، $157 = 31(5)+2$ ، $157 = (22)(7)+3$ ، $157 = 14(11)+3$ ، وبالتالي فإن 157 لا يقبل القسمة على أي من $2,3,5,7,11$. أما $10 < \sqrt{85} < 9$ ، وعليه فإن $(10)^2 - 85 = 15$ ، $11^2 - 85 = 121 - 85 = 36$ ، وعليه فإن $85 = 11^2 - 6^2 = (11+6)(11-6) = 17 \times 5$. إذاً

$$n = 13345 = 157 \times 17 \times 5$$

تمارين

(١) أثبت أن كلاً من $197,239,313,461$ عدد أولي .

(٢) أوجد الأعداد الأولية الواقعة بين 270، 320 .

(٣) أثبت صحة حدس جولباخ لكل من الأعداد الآتية $32,98,460,1024$.

(٤) إذا كان $a,b,c,d \in Z$ وكان p عدداً أولياً ، و $ab = cd$ ، $p \backslash a$ فأثبت أن $p \backslash c$ أو $p \backslash d$.

(٥) إذا كان $n > 1$، فأثبت أن $n^4 + 4$ عدد مؤلف .

(٦) إذا كان $p \geq 5$ عدداً أولياً ، فأثبت أن $p^2 + 2$ عدد مؤلف " لاحظ أن أما $p = 6m+1$ أو $p = 6m+5$ "

(٧) برهن على وجود عدد لا نهائي من الأعداد الأولية على الصورة $6r-1$ ، $r \in N^*$. " ملاحظة : أفرض وجود عدد منتهي $p_1,\cdots,p_n$ من تلك الأعداد وضع $m = 6(p_1 \cdots p_n) - 1$ ، وأثبت أن $p \backslash m$ لكن $p \neq p_i$ لكل $i = 1,\cdots,n$.

(٨) إذا كان p عدداً أولياً فردياً لا يساوي 5 ، فأثبت أن $10\backslash p^2-1$ أو $10\backslash p^2+1$. " لاحظ أن $p\in\{5m+1, 5m+2, 5m+3, 5m+4\}$

(٩) إذا كان p عدداً أولياً وكان $p\backslash a^n$ ، فأثبت أن $p^n\backslash a^n$.

(١٠) إذا كان $p\geq q\geq 5$ عددين أوليين ، فأثبت أن $24\backslash p^2-q^2$.

(١١) حقق تخمين لاجرانج لكل الأعداد الفردية الأكبر من 5 وأقل من 37 .

(١٢) أُثبتَ عام ١٩٥٠م أنه يمكن التعبير عن أي عدد صحيح أكبر من 9 كمجموع أعداد أولية فردية . عبر عن كل من الأعداد 25,69,81,125 كمجموع أعداد أولية فردية .

(١٣) أستخدم طريقة فيرما لتحليل كل من الأعداد الآتية إلى عواملها الأولية 237 ، 343 ، 1745 ، 18531 .

(١٤) أثبت أن 307 عدد أولي ، ثم أثبت أنه كان $(1\times2\times3\times\cdots\times99)n=307\times306\times\cdots\times209$ ، فأن $307\backslash n$.

٢-٣ : المبرهنة الأساسية في الحساب وبعض تطبيقاتها

تنص المبرهنة الأساسية في الحساب على إمكانية تحليل أي عدد صحيح أكبر من الواحد (بطريقة وحيده) إلى عوامله الأولية .

ويعتقد البعض بأن القضية الرابعة عشرة (IX−14) في الجزء التاسع من كتاب الأصول " **إذا كان عدد ما هو أقل عدداً تعدّه أعداد أولية ، فلا يعده أي عدد أولي آخر غير هذه الأعداد التي تعدّه** "بأنها المبرهنة الأساسية في الحساب لكن تلك القضية تكافئ قولنا أن المضاعف المشترك الأصغر لأعداد أولية لا يقبل قواسم أولية إلا تلك الأعداد وهذه ليست المبرهنة الأساسية بأي حال من الأحوال لأنه لا الفارسي ولا الكرخي ولا شراح إقليدس ممن هم بتميز ابن الهيثم قد تعرفوا في القضية (IX−14) إلى ما سوف يصبح لاحقاً المبرهنة الأساسية

أنظر [٦ ، ص ٣١٩-٣٢٢] ، هذا ويؤكد كل من هاردي ورايت عام (١٩٣٨م) عدم ذكر إقليدس لأي نص للمبرهنة الأساسية ، كما تؤكد بورباكي الفرنسية في (أسس الرياضيات ص ١١٠) أن إقليدس لم يتمكن من صياغة هذه المبرهنة بسبب نقص المصطلحات والرموز المناسبة للقوى من أية درجة كانت . ويقول الألماني إيتارد في كتابه (الحساب عند إقليدس ص ٨٦) يجب أن لا نبحث في كتاب الأصول عن التبديل ولا عن التجميع في حاصل ضرب عدة عوامل ، ولا عن تحليل العدد إلى عوامله الأولية ولا عن كافة قواسمه .

إذاً المبرهنة الأساسية ليست لإقليدس بل هي لرياضي آخر هو كمال الدين الفارسي ، وردت في بحثه " تذكرة الأحباب في تمام التحاب " للتمكن من إدخال الطرق التوافقية ومعرفة القواسم الفعلية لعدد . ونورد فيما يأتي نص الفارسي وإثباته لتلك المبرهنة [٣ أو ٤ ، ص ٣١٨] .

" كل مؤلف فإنه لابد وأن ينحل إلى أضلاع أوائل متناهية هو متآلف من ضربها بعضها في بعض .

أي أن كل عدد طبيعي يمكن التعبير عنه كحاصل ضرب عدد منتهي من الأعداد الأولية " .

<u>البرهان:</u> (الفارسي)

ليكن n عدداً طبيعياً أكبر من الواحد وله قاسم أولى p_1 . إذاً $n = ap_1$ ، $1 \leq a < n$ حسب القضية الثالثة عشر في الجزء الثامن من الأصول لإقليدس ، فإذا كان a عدداً أولياً فقد انتهى البرهان ، وإلا كان للعدد a قاسم أولى p_2 بحيث أن $a = bp_2$ ، $1 \leq b \leq a$ فإذا كان b عدداً أولياً ، فإن $n = bp_1 p_2$ ، وأنتهى البرهان ، وإلا فإننا نكرر الطريقة نفسها لعدد منتهي من المرات حتى نصل إلى عدد أولى p_r بحيث أن $n = p_1 p_2 \cdots p_r$.

ويكتب الفارسي **" وإن لم ينحل إلى ضلعين أولين أبداً لزم تأليف المتناهي من ضرب المتناهي من ضرب أعداد غير منتهية بعضها في بعض وهذا محال "**

وهكذا بعد أن يثبت الفارسي وجود تحليل بعد منتهي من العوامل الأولية يحاول بطريقة غير موفقة أن يثبت وحدانية التحليل ولا نجد إثباتاً تاماً للمبرهنة الأساسية في الحساب إلا عام ١٨٠١م عند الألماني جاوس (١٧٧٧-١٨٥٥م) .

لاحظ أن وحدانية التحليل (Unique factorization) ، تحتاج إلى أثبات ، لأنها قد لا تتحقق في بعض المجموعات العددية ، فمثلاً إذا كانت $S=\{4m+1 | m\in N\}$ ، وعرفنا العدد الأولي في S بأنه ذلك العدد الأكبر من الواحد ولا يقبل القسمة إلا على نفسه والواحد ، فإن كلاً من $5,9,21,33,49,77\in S$ عدد أولي بينما $25\in S$ عدد مؤلف كما أن $441=9\times 49=21\times 21$ ، $693=21\times 33=9\times 77$.

والآن إلى طريقة أخرى لإثبات التحليل إلى العوامل الأولية وإثبات وحدانيته .

مبرهنة ٢-٣-١ : " المبرهنة الأساسية في الحساب

" The Fundamental Theorem of Arithmatic

يمكن التعبير بطريقة وحيدة (عدا الترتيب) عن أي عدد صحيح أكبر من الواحد كحاصل ضرب عدد منتهي من الأعداد الأولية .

البرهان: (بالاستقراء الرياضي)

نفرض أن $1<n\in Z$. إذاً عندما $n=2$ ، فقد تم المطلوب لآن 2 عدد أولي . والآن لنفرض أن العبارة صحيحة لكل $2\le m\le n$ ولإثبات صحتها عندما $n=m+1$. لاحظ أن إذا كان $m+1$ عدداً أولياً فقد تم المطلوب ، أما إذا كان $m+1$ عدداً مؤلفاً ، فيوجد $a,b\in Z$ بحيث أن $m+1=ab$ ، $1<a<m+1$ ، $1<b<m+1$ ، حسب مبرهنة (٢-٢-١) . لكن كلاً من a,b يمكن التعبير عنه كحاصل ضرب منتهي من الأعداد الأولية حسب فرضية الاستقراء الرياضي. إذاً يمكن التعبير عن $(m+1)$ كحاصل ضرب أعداد أولية، وعليه فإن العبارة صحيحة عندما $n=m+1$. إذاً العبارة صحيحة لكل $n>1$.

ولإثبات وحدانية التعبير نفرض أن $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ حيث p_i , q_j أعداد أولية لجميع قيم $1 \le i \le r$ ، $1 \le j \le s$. سنثبت بالاستقراء الرياضي على r بأن $r = s$ ، $p_i = q_i$ لكل i . فإذا كان $r = 1$ فإن $n = p_1 = q_1 (q_2 \cdots q_2)$ لكن p_1 عدد أولي ، إذاً $s = 1$ ، $p_1 = q_1$. والآن لنفرض أن $r > 1$ وأنه عندما يعبر عن n كحاصل ضرب أعداد أولية عددها أقل من r يكون ذلك التعبير وحيداً . وحيث أن $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ يعني أن $p_1 \backslash (q_1 \cdots q_s)$. إذاً يوجد $1 \le m < s$ بحيث أن $p_1 \backslash q_m$ حسب مبرهنة (٢-٢-٣ب) وحيث أنه يمكن أن نفرض دون التأثير على عمومية البرهان أن $p_1 \backslash q_1$ فنجد أن $p_1 = q_1$ لآن q_1 عدد أولي. لكن $p_1 = q_1$ يعني أن $p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$. وعليه فإن عدد عوامل الطرف الأيسر من هذه المعادلة يساوي $(r-1)$. إذاً $p_2 = q_3 , p_3 = q_3 , \cdots , q_s$ حسب فرضية الأستقراء الرياضي .

□

ملاحظة :

(أ) بما أن بعض الأعداد الأولية التي تظهر عند التعبير عن أي عدد صحيح أكبر من الواحد تكون متساوية . إذاً يمكن التعبير بطريقة وحيدة (عدا الترتيب) عن أي عدد صحيح $n > 1$ بالصورة الآتية ، والتي تسمى الصورة القياسية $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ ، حيث p_i أعداد أولية مختلفة لكل $i = 1 , \cdots , r$.

(ب) إذا كان $n < (-1)$ ، فإن $-n > 1$ وعليه يمكن التعبير عن $-n$ بطريقة وحيدة كحاصل ضرب أعداد أولية ، إذاً $-n = \prod_{i=1}^{s} p_i^{\alpha_i}$ ، وعليه فإن $n = (-1) \prod_{i=1}^{s} p_i$ حيث p_i أعداد أولية مختلفة لجميع قيم $1 \le i \le s$.

ومن (أ) ، (ب) نجد أنه إذا كان $n \in Z - \{-1,0,1\}$ ، فيمكن التعبير عن n كحاصل ضرب أعداد أولية .

مثال (١) :

(أ) $90 = 2 \times 3^2 \times 5$ ، (ب) $720 = 2^4 \times 3^2 \times 5$

(ج) $-138600 = (-1) \times 2^3 \times 3^2 \times 5 \times 7 \times 11$.

والآن إلى بعض تطبيقات المبرهنة الأساسية في الحساب .

مبرهنة ٢-٣-٢ :

إذا كان a,b عددين صحيحين ، $(a,b) = 1$ وكان c قاسماً موجباً للعدد ab فيوجد عددان موجبان وحيدان d,e بحيث أن

(أ) $c = de$ و $(d,e) = 1$ ، (ب) $d \backslash a$ و $e \backslash b$.

البرهان :

بما أن $a = \prod_{i=1}^{n} p_i^{r_i}$ ، $b = \prod_{j=1}^{m} q_j^{s_j}$ حسب المبرهنة الأساسية ، وبما أن $(a,b) = 1$. إذاً $p_i \neq q_j$ لكل i,j ، وعليه فإن $ab = (\prod_{i=1}^{n} p_i^{r_i})(\prod_{j=1}^{m} q_j^{s_j})$

لكن $c \backslash ab$ ، بالفرض . إذاً $c = \prod_{i=1}^{n} p_i^{\alpha_i} \cdot \prod_{j=1}^{m} q_j^{\beta_j}$ ، حيث $0 \leq \alpha_i \leq r_i$ ، $0 \leq \beta_j \leq s_j$ لكل $1 \leq i \leq n$ ، $1 \leq j \leq m$. والآن إذا كان

$d = \prod_{i=1}^{n} p_i^{\alpha_i}$ ، $e = \prod_{j=1}^{m} q_j^{\beta_j}$ ، فإن $c = de$ و $(d,e) = 1$ و $d \backslash a$ ، $e \backslash b$

ولإثبات وحدانية d,e نفرض $c = de = rs$ و $(d,e) = 1$ ، $(r,s) = 1$ ، $d \backslash a$ ، $r \backslash a$ ، $e \backslash b$ ، $s \backslash b$.

سنثبت أن $(d,s)=1$ ولإثبات ذلك نفرض أن $(d,s)\neq 1$. إذاً يوجد عدد أولي p بحيث أن $p\setminus d$ ، $p\setminus s$ حسب مبرهنة (٢-٢-٤أ) . لكن $d\setminus a$ و $s\setminus b$. إذاً $p\setminus a$ و $p\setminus b$ ، وعليه فإن $(a,b)\neq 1$ وهذا خلاف الفرض . إذاً $(d,s)=1$ ، وعليه يوجد $x,y\in Z$ بحيث أن $dx+sy=1$ ، وبالتالي فإن $rdx+rsy=r$ و $d\setminus rs$. إذاً $d\setminus r$. وبنفس الطريقة يمكن أن نبرهن على أن $r\setminus d$. لكن كلاً من r,d عدد صحيح موجب . إذاً $r=d$ ، وعليه فإن $e=s$.

□

مبرهنة ٢-٣-٣ :

إذا كان a,n عددين صحيحين ، فإن $\sqrt[n]{a}$ عدد نسبي إذاً وإذا فقط كان $\sqrt[n]{a}$ عدداً صحيحاً .

البرهان :

إذا كان $\sqrt[n]{a}$ عدداً صحيحاً ، فمن البديهي أن $\sqrt[n]{a}$ عدد نسبي . ولإثبات العكس نفرض أن $\sqrt[n]{a}$ عدد نسبي . إذاً يوجد $b,c\in Z$ بحيث أن $\sqrt[n]{a}=\dfrac{b}{c}$ و $(b,c)=1$. لكن $a=\dfrac{b^n}{c^n}$ ، وبالتالي فإن $b^n=ac^n$ ، وعليه فإن $c\setminus b^n$.
فإذا كان $c\neq\mp 1$ ، فيوجد عدد أولي p بحيث أن $p\setminus c$ حسب المبرهنة الأساسية في الحساب ، وعليه فإن $p\setminus b^n$ ، وبالتالي فإن $p\setminus b$ حسب مبرهنة (٢-٢-٣ب) . إذاً $(b,c)\geq p\neq 1$ وهذا يناقض كون $(b,c)=1$. إذاً $c=\mp 1$، وعليه فإن $\sqrt[n]{a}=b$ عدد صحيح .

□

مثال (٢) :

$\sqrt{2}$ ، $\sqrt[3]{30}$ ، $\sqrt[5]{6}$ ، $\log_6 3$ أعداد غير نسبية .

الحل :

(أ) بما أن $1<\sqrt{2}<2$ ولا يوجد عدد صحيح بين 1 ، 2 حسب مبرهنة (١-٢-١ج) . إذاً $\sqrt{2}$ عدد غير نسبي حسب مبرهنة (٢-٣-٤) .

(ب) بما أن $4 < \sqrt[3]{30} < 3$ ولا يوجد عدد صحيح بين 3 ، 4 حسب مبرهنة (١-٢-١ج) . إذاً $\sqrt[3]{30}$ عدد غير نسبي حسب مبرهنة (٢-٣-٤) .

(ج) بما أن $2 < \sqrt[5]{6} < 1$ ولا يوجد عدد صحيح بين 1 ، 2 . إذاً $\sqrt[5]{6}$ عدد غير نسبي حسب مبرهنة (٢-٣-٤) .

(د) نفرض أن $\log_6(3) = \frac{a}{b}$ ، $a,b \in Z$ ، $b \neq 0$. إذاً $6^a = 3^b$ ، وعليه فإن $2^a \cdot 3^a = 3^b$ وهذا يناقض وحدانية التحليل في المبرهنة الأساسية في الحساب . إذاً $\log_6(3)$ عدد غير نسبي .

□

والآن إلى تعريف ودراسة خواص المضاعف المشترك البسيط .

تعريف ١ :

يقال عن $m \in Z^+$ ، أنه مضاعف مشترك أصغر أو بسيط (Least common multiple) للأعداد $a_1, a_2, \cdots, a_n \in Z^*$ ، إذا كان :

(أ) $a_i \backslash m$ لكل $i = 1, \cdots, r$.

(ب) إذا كان $c > 0$ ، $a_i \backslash c$ لكل $i = 1, \cdots, r$ ، فإن $m \backslash c$.

يعبر عادة عن المضاعف المشترك البسيط للأعداد $a_1, \cdots, a_r$ بالشكل $[a_1, a_2, \cdots, a_n]$ أو $\text{l.c.m}(a_1, a_2, \cdots, a_n)$. ويمكن أن نبرهن على أن المضاعف المشترك البسيط لأي عددين غير صفريين أو أكثر يكون وحيداً .

مثال (٣) :

(أ) $[4,15] = 60$.

(ب) إذا كان $a = 195$ ، $b = -273$ ، فإن $a = 3 \times 5 \times 13$ ، $b = (-1) \times 3 \times 7 \times 13$ ، وعليه فإن $[a,b] = 3 \times 5 \times 7 \times 13 = 1365$.

(ج) إذا كان $a=-1287$ ، $b=-507$ ، فإن $a=(-1)3^2\times 11\times 13$ ، أما $b=(-1)\times 3\times 13^2$ ، وعليه فإن $[a,b]=3^2\times 11\times 13^2$ ، وبصورة عامة نجد أن $[a,b]=[-a,b]=[a,-b]=[-a,-b]$.

(د) لإيجاد القاسم المشترك الأعظم والمضاعف المشترك البسيط للعددين 1176 ، 936 . لاحظ أن $1176=2^2\times 3\times 7^2$ ، $936=2^2\times 3^2\times 13$.
إذاً $(a,b)=2^2\times 3=24$ ، بينما $[a,b]=2^3\times 3^2\times 7^2\times 13$ ، وبصورة عامة إذا كان $a=\prod_{i=1}^{n} p_i^{r_i}$ ، $b=\prod_{i=1}^{n} p_i^{s_i}$ ، فإن

$$[a,b]=\prod_{i=1}^{n} p_i^{\max\{r_i,s_i\}} \quad ، \quad (a,b)=\prod_{i=1}^{n} p_i^{\min\{r_i,s_i\}}$$

والآن إلى خواص المضاعف المشترك البسيط والمبرهنات الآتية "

مبرهنة ٢-٣-٤ : ليكن $a,b,c\in Z$.

(أ) إذا كان $c>0$ ، فإن $[ac,bc]=c[a,b]$.

(ب) $[a,b]\cdot(a,b)=|ab|$.

البرهان :

(أ) نفرض أن $n=[ac,bc]$ ، $m=[a,b]$. إذاً cm من مضاعفات ac ، bc وعليه فإن cm يقبل القسمة على n وهذا يعني أن $cm\geq n$ لكن $\frac{\frac{n}{c}}{a}=\frac{n}{bc}$ ، $\frac{\frac{n}{c}}{a}=\frac{n}{ac}$ ، وعليه فإن $\frac{n}{c}$ يقبل القسمة على كل من a,b ، وبالتالي فإن $\frac{n}{c}$ يقبل القسمة على m ، وعليه فإن $\frac{n}{c}\geq m$ ، ومنها نجد أن $n\geq cm$.
إذاً $n=cm$.

(ب) بما أن $[a,b]=[a,-b]=[-a,b]=[-a,-b]$ ، إذاً يكفي أن نبرهن النتيجة عندما $a,b\in N^*$ ، ولإثبات ذلك نفرض أن $d=(a,b)$. إذاً $d\backslash a$ ، $d\backslash b$ ، وعليه يوجد $r,s\in N$ بحيث أن $a=dr$ ، $b=ds$.

والآن لنفرض أن $m=\frac{ab}{d}$ ، إذاً $m=as=br$. وإذا كان $a\backslash c$ ، $b\backslash c$ فإن $c=au=bv$ حيث أن $u,v\in N$. لكن $d=(a,b)$. إذاً يوجد $x,y\in Z$ بحيث أن $d=ax+by$ ، وعليه فإن

$$\frac{c}{m}=\frac{cd}{ab}=\frac{c(ax+by)}{ab}=\frac{c}{b}x+\frac{c}{a}y=vx+uy$$

إذاً $m\backslash c$ ، وعليه فإن $m\leq c$ ، وبالتالي فإن $m=[a,b]$ ، ومنها نجد أن $[a,b]\cdot(c,d)=ab$.

□

نتيجة :

$[a,b]=|ab|$ إذاً وإذا فقط كان $(a,b)=1$.

البرهان :

طبق مبرهنة (٢-٣-٤ب) تحصل على المطلوب .

□

ملاحظة :

إذا كان $a,b,c\in Z$ ، فإن $[a,b,c]\cdot(a,b,c)\neq|abc|$ ، كما يوضح ذلك المثال الآتي :

لتكن $a=18$ ، $b=24$ ، $c=36$. إذاً $a=2\times3^2$ ، $b=2^3\times3$ ، $c=2^2\times3^2$ ، وعليه فإن $[a,b,c]=2^3\times3^2$ ، $(a,b,c)=2\times3$ ، $[a,b,c]\cdot(a,b,c)=2^4\times3^3$ ، $abc=2^6\times3^5$ ، وبالتالي فإن $[a,b,c]\cdot(a,b,c)\neq abc$.

وأخيراً إلى المبرهنة الآتية التي توضح كيفية إيجاد المضاعف المشترك البسيط لأكثر من عددين .

مبرهنة ٢-٣-٥ :

ليكن $0 \neq a_i \in Z$ لكل $i = 1, \cdots, n$ ، فإن

$$[a_1, a_2, \cdots, a_{n-1}, a_n] = [[a_1, \cdots, a_{n-1}], a_n]$$

البرهان :

نفرض أن $m = [a_1, a_2, \cdots, a_n]$ ، $r = [a_1, \cdots, a_{n-1}]$ ، $s = [r, a_n]$. إذاً $r \backslash s$ و $a_i \backslash r$ لكل $i = 1, \cdots, n-1$ وبالتالي فإن $a_i \backslash s$ لكل $i = 1, \cdots, n-1$ ، لكن $a_n \backslash s$ ، إذاً $a_i \backslash s$ لكل $i = 1, \cdots, n$. وحيث أن $m = [a_1, \cdots, a_n]$ ، إذاً $m \backslash s$ ، وعليه فإن $m \leq s$. والآن $a_i \backslash m$ لكل $i = 1, \cdots, n-1$ و $r = [a_1, \cdots, a_{n-1}]$ يعني أن $r \backslash m$. لكن $a_n \backslash m$ و $s = [r, a_n]$. إذاً $s \backslash m$ وعليه فإن $s \leq m$. وبالتالي فإن $m = s$.

مثال (٤) :

أوجد المضاعف المشترك البسيط للأعداد $234, 192, 345$.

الحل :

بما أن $[234, 192, 345] = [[234, 192], 345]$ ، $234 = 2 \times 3^2 \times 13$ ، $192 = 2^6 \times 3$. إذاً $[234 و 192] = 2^6 \times 3^2 \times 13$. لكن $345 = 3 \times 5 \times 23$ ، إذاً $m = [[234, 192], 345] = 2^6 \times 3^2 \times 5 \times 13 \times 23$.

لاحظ أنه يمكن حساب المضاعف المشترك البسيط كالآتي :

2	234	192	345
2	117	96	345
2	117	48	345
2	117	24	345
2	117	12	345
2	117	6	345
3	117	3	345
3	39	1	115
5	13	1	115
13	13	1	23
23	1	1	23
	1	1	1

إذاً $[234,192,345]=2^6\times3^2\times5\times13\times23$.

تمـــــــارين

(١) أوجد القاسم المشترك الأعظم والمضاعف المشترك البسيط للعددين a,b عندما :

(أ) $a=3997$ ، $b=2947$.

(ب) $a=11328$ ، $b=5421$.

(ج) $a=2^{30}\cdot5^{21}\cdot19\cdot(23)^3$ ، $b=2^6\cdot3\cdot7^4\cdot(19)^3\cdot(23)^7$

(٢) أوجد القاسم المشترك الأعظم والمضاعف المشترك البسيط للأعداد a,b,c عندما :

(أ) $a=1128\ ,\ b=936\ ,\ c=648$.

(ب) $a=26542\ ,\ b=10190\ ,\ c=1234$.

(٣) أوجد $[18,28,20,35]$ ، $[1176,588,492,1024]$.

(٤) أثبت أن $\sqrt[3]{2}$ ، $\sqrt{68}$ ، $\sqrt[6]{21}$ ، $\log_{10}(4)$ أعداد نسبية .

(٥) أثبت بإستخدام المبرهنة الأساسية في الحساب أن :

(أ) إذا كان $a,b,c\in Z$ وكان $a\setminus c$ ، $b\setminus c$ ، $(a,b)=1$ ، فإن $ab\setminus c$.

(ب) إذا كان $a,b,c,d\in Z$ وكان $ab\setminus cd$ و $(a,b)=1$ فإن $a\setminus c$.

(٦) إذا كان a,b عددين صحيحين موجبين وكان $(a,b)=1$ و $c^n=ab$ فبرهن على وجود عددين صحيحين e,d بحيث أن $a=d^n$ ، $b=e^n$.

(٧) إذا كان $a,b,c\in Z$ وكان $b\setminus c$ ، فأثبت أن $[a,b]\leq[a,c]$.

(٨) إذا كان $a,b\in Z^*$ ، فأثبت أن $b\setminus a \Leftrightarrow [a,b]=|a|$.

(٩) إذا كان $a,b,c\in Z$ ، فأثبت أن $\left([a,b],c\right)=[(a,c),(b,c)]$ ، وحقق ذلك عندما $a=120$ ، $b=270$ ، $c=225$.

(١٠) إذا كان a,b,c,m,r,v أعداداً صحيحة موجبة وكان $[a,b]=m$ ، $a=rb+c$ ، $m=vc$ ، فأثبت أن :

(أ) يوجد $u\in Z$ بحيث أن $vc=ub$ ، (ب) $b\setminus va$.

(ج) $[a,b]\setminus va$ ، (د) $va=[a,b]$

(١١) إذا كان $a,b,c\in Z$ ، فأثبت أن $[a,b,c](ab,ac,bc)=|abc|$ ، وحقق ذلك عندما $a=24$ ، $b=60$ ، $c=14$.

(١٢) إذا كان $a,b,c\in Z$ ، فأثبت أن $[a,b,c]\cdot(a,b,c)\le|abc|$

(١٣) إذا كان $a,b,c\in Z$ ، وكان $[a,b,c]\cdot(a,b,c)=|abc|$ ، فأثبت أن $(a,b)=(b,c)=(a,c)=1$

****

الفصل الثالث

التطابقات (Congruences)

التطابق هو تعبير آخر لمفهوم القسمة ، قُدّم من قبل الألماني جاوس (١٧٧٧-١٨٥٥م) عام ١٨٠١م بطريقة جعلته أداة فعالة لتسهيل البراهين ووسيلة أخرى لدراسة نظرية الأعداد ويضم هذا الفصل ستة بنود ندرس فيها تعريف التطابق وخواصه الأساسية وبعض تطبيقاته وفصول التطابق وأنظمة البواقي التامة والمختزلة ، التطابقات الخطية ومبرهنة الباقي الصينية ومبرهنتي أويلر وفيرما ومبرهنة ابن الهيثم (ولسن) .

٣-١ : مفهوم التطابق وخواصه الأساسية

سنركز اهتمامنا في هذا الجزء على تعريف التطابق ودراسة خواصه الأساسية .

تعريف ٣-١-١ :

إذا كان $n\in N^*$ ، $a,b\in Z$ ، فيقال عن a أنه يطابق أو يوافق b (Congruent) قياس n (modulo) ، ونكتب $a\equiv b(\text{mod } n)$ أو $a\equiv_n b$ إذا كان $a-b$ يقبل القسمة على n .

إذا كان a لا يطابق b قياس n ، فيعبر عن ذلك بالشكل $a\not\equiv b(\text{mod } n)$.

مثال (١) :

(أ) $31\equiv 1(\text{mod}.2)$ ، لأن $31-1=30$ يقبل القسمة على 2 .

(ب) $31\not\equiv 1(\text{mod } 4)$ ، لأن $31-1=30$ يقبل القسمة على 4 .

تعريف ٣-١-٢ :

يقال أن a قياس n يساوي r ، ونكتب $a\,(\text{mod } n)=r$ ، إذا كان $a=ns+r$ ، $0\le r<n$.

مثال (١) :

(أ) $5(\bmod 3)=2$ ، لأن $5=1\times3+2$ ، $2\bmod 3=2$ ، لأن $2=0\times3+2$ ، $3\bmod 3=0$ ، لأن $3=1\times3+0$.

(ب) $31\equiv1(\bmod 3)$ و $31(\bmod 3)=1$ ، لأن $31=10\times3+1$
$4(\bmod 3)=1$ ، لأن $4=1\times3+1$ ، وعليه فإن
$31(\bmod 3)=4(\bmod 3)$.

وبصورة عامة يمكن أن نبرهن ما يلي .

مبرهنة ٣-١-١ :

إذا كان $n\in N^*$ ، $a,b\in Z$ ، فإن $a\equiv b(\bmod n)$ ، إذاً وإذا فقط كان $a\ (\bmod n)=b(\bmod n)$. أي أن

$$a\equiv b(\bmod n) \Leftrightarrow (\text{باقي قسمة } a \text{ على } n) = (\text{باقي قسمة } b \text{ على } n)$$

البرهان :

نفرض أن $a\equiv b(\bmod n)$ ، إذاً $n\backslash a-b$ ، وعليه يوجد $r\in Z$ بحيث أن $a=b+nr$. لكن $b,n\in Z$ إذاً بإستخدام القسمة الخوارزمية يمكننا أن نوجد $m,s\in Z$ بحيث أن $b=mn+s$ ، $0\le s<n$ ، وعليه فإن $a=(m+r)n+s$ ، $(m+r)\in Z$. إذاً باقي قسمة a على n يساوي باقي قسمة b على n ، وعليه فإن $a\ (\bmod n)=b(\bmod n)$.

ولإثبات العكس نفرض أن $a\ (\bmod n)=b(\bmod n)$. إذاً $a=nr+t$ ، $b=ns+t$ ، وبالتالي فإن $a-b=(r-s)n$ ، $r-s\in Z$ وهذا يعني أن $n\backslash a-b$ ، وعليه فإن $a\equiv b(\bmod n)$.

□

وقبل دراسة الخواص الأخرى لعلاقة التطابق نورد ما يلي :

تعريف ٣-١-٣ :

يقال عن علاقة R على مجموعة A أنها علاقة تكافؤ (Equivalence Relation) على A ، إذا كان :

(أ) R علاقة منعكسة (reflexive) على A ، أي أن $\forall a \in A , aRa$.

(ب) R علاقة متناظرة (symmetric). أي أن إذا كان $a,b \in A$ وكان aRb، فإن bRa .

(ج) R علاقة متعدية (transitive) . أي أن إذا كـــان $a,b,c \in A$ ، aRb و bRa فإن aRc .

مثال (٣) :

(أ) إذا كانت $A = \{1,2,3\}$ ، فإن كـــلاً مـــن $R_1 = \{ (1,1),(2,2),(3,3)\}$ ،
$R_2 = \{ (1,1),(2,2),(3,3),(1,2),(2,1) \}$ ،
$R_3 = \{ (1,1),(2,2),(3,3),(1,3),(3,1) \}$ ،
$R_4 = \{ (1,1),(2,2),(3,3),(2,3),(3,2) \}$ ،
$R_5 = \{ (1,1),(2,2),(3,3),(1,2),(2,1),(1,3),(3,1),(2,3),(3,2) \}$
علاقة تكافؤ على A .

(ب) إذا كان $A = Z$ وكانت R معرفة كالآتي : $a,b \in Z , aRb \Leftrightarrow |a| = |b|$
فإن R علاقة تكافؤ على Z .

والآن إلى المبرهنة الآتية :

مبرهنة ٣-٢-٢ :

التطابق قياس n علاقة تكافؤ على Z . أي أن :

(أ) $a \equiv a (\text{mod } n)$ لكل $a \in Z$.

(ب) إذا كان $a,b \in Z$ ، وكان $a \equiv b(\text{mod } n)$ ، فإن $b \equiv a(\text{mod } n)$.

(ج) إذا كان $a,b,c \in Z$ ، وكان $b \equiv c(\text{mod } n)$ ، $a \equiv b(\text{mod } n)$ ، فإن $a \equiv c \text{ mod } n$.

البرهان :

(أ) بما أن $a-a=0$ لكل $a\in \mathbb{Z}$ ، وبما أن $n \backslash 0$ لكل $n\neq 0$. إذاً $a\equiv a$ لكل $a\in \mathbb{Z}$.

(ب) بما أن $a\equiv b(\bmod n)$. إذاً $n \backslash a-b$ ، وعليه يوجد $r\in \mathbb{Z}$ بحيث أن $a-b=nr$ ، وعليه فإن $b-a=n(-r)$ ، $-r\in \mathbb{Z}$ ، وبالتالي فإن $b\equiv a(\bmod n)$.

(ج) بما أن $a\equiv b(\bmod n)$ و $b\equiv c(\bmod n)$. إذاً يوجد $r,s\in \mathbb{Z}$ بحيث أن $a-b=nr$ ، $b-c=ns$ ، ومنهما نجد أن $a-c=n(r+s)$. لكن $r,s\in \mathbb{Z}$. إذاً $a\equiv c(\bmod n)$.

□

مبرهنة ٣-١-٣ :

إذا كان $a,b,c,d\in \mathbb{Z}$ وكان $n\in \mathbb{N}^*$ ، $a\equiv b(\bmod n)$ ، $c\equiv d \bmod n$ ، فإن :

(أ) $a\mp c\equiv b\mp d(\bmod n)$ ، (ب) $ac\equiv bd(\bmod n)$

(ج) $a+e\equiv b+e(\bmod n)$ لكل $e\in \mathbb{Z}$ ، (د) $ae\equiv be(\bmod n)$ لكل $e\in \mathbb{Z}$

(هـ) $ar+cs\equiv br+ds$ لكل $r,s\in \mathbb{Z}$.

البرهان :

(أ) ، (ب) بما أن

$$a\equiv b(\bmod n)\Rightarrow \exists x\in \mathbb{Z} :\ a=b+nx\ \ldots (1)$$

$$c\equiv d(\bmod n)\Rightarrow \exists y\in \mathbb{Z} :\ c=d+ny\ \ldots (2)$$

إذاً بجمع المعادلتين (1) ، (2) ينتج أن $a+c=b+d+n(x+y)$ لكن $x+y\in \mathbb{Z}$. إذاً $a+c\equiv b+d(\bmod n)$.

وبطرح المعادلة (2) من (1) ينتج أن $a-c=b-d+n(x-y)$ ، $x-y\in \mathbb{Z}$. إذاً $a-b\equiv c-d(\bmod n)$.

وبضرب المعادلتين (1) ، (2) ينتج أن $ac = bd + n(by + xd + nxy)$ لكن $by + xd + nxy \in Z$. إذاً $ac \equiv bd \pmod n$.

(ج) ، (د) بما أن $a \equiv b \bmod n$ ، $e \equiv e \pmod n$ لكل $e \in Z$. إذاً $a + e \equiv b + e \pmod n$ و $ae \equiv be \pmod n$ حسب (أ ، ب) .

(هـ) بما أن $a \equiv b \pmod n$ ، $c \equiv d \pmod n$ بالفرض.إذاً $ar \equiv dr \pmod n$ و $cs \equiv ds \pmod n$ لكل $r, s \in Z$ حسب (د) ، وعليه فإن $ar + cs \equiv br + ds \pmod n$ حسب (أ) .

□

ملاحظة :

إذا كان $ac \equiv bc \pmod n$ ، فإن $a \not\equiv b \pmod n$ ، كما يوضح ذلك المثال الآتي : $7 \times 4 \equiv 6 \times 4 \pmod 2$ بينما $7 \not\equiv 6 \pmod 2$. لكن يمكن أن نبرهن ما يلي :

مبرهنة ٣-١-٤ :

إذا كان $a, b, c \in Z$ وكان $n \in N^*$ ، $d = (c, n)$ ، فإن $ac \equiv bc \pmod n$ إذاً وإذا فقط كان $a \equiv b \bmod (\frac{n}{d})$.

البرهان :

نفرض أن $ac \equiv bc \pmod n$. إذاً يوجد $r \in Z$ بحيث أن $(a - b)c = ac - bc = nr$ ، وعليه فإن $(a - c)\frac{c}{d} = \frac{n}{d}r$. لكن $d = (c, n)$. إذاً $(\frac{c}{d}, \frac{n}{d}) = 1$ حسب نتيجة(١) من المبرهنة (٢-١-٨)، وعليه فإن $a - b = \frac{nr}{d}$ حسب مبرهنة (٢-١-٩ب) وهذا يعني أن $a \equiv b \bmod (\frac{n}{d})$

ولإثبات العكس نفرض أن $a \equiv b \bmod (\frac{n}{d})$. إذاً يوجد $r \in Z$ بحيث أن

$a-b=\frac{nr}{d}$ ، وعليه فإن $ac-bc=\frac{ncr}{d}$. لكن $d\backslash c$ ، إذاً يوجد $s\in Z$ بحيث أن $c=ds$ ، وعليه فإن $ac-bc=n(rs)$ ، $rs\in Z$ وهذا يعني أن $ac\equiv bc(\text{mod } n)$.

□

نتيجة :

إذا كان $a,b,c\in Z$ ، $n\in N^*$ وكان $ac\equiv bc(\text{mod } n)$ ، $(c,n)=1$ ، فإن $a\equiv b(\text{mod } n)$.

البرهان :

يترك للقارئ . □

مبرهنة ٣-١-٥ :

إذا كان $a_i\equiv b_i\,(\text{mod } n)$ ، لكل $i=1,\cdots,m$ ، فإن :

(أ) $\sum_{i=1}^{m} a_i\equiv\sum_{i=1}^{m} b_i\,(\text{mod } n)$ ، (ب) $\prod_{i=1}^{m} a_i\equiv\prod_{i=1}^{m} b_i$

البرهان : (بالأستقراء على m) وسنثبت (أ) ونترك (ب) للقارئ .

(أ) لتكن $P(m):\sum_{i=1}^{m} a_i\equiv\sum_{i=1}^{m} b_i\,(\text{mod } n)$. إذاً عندما $m=1$ نجد أن $a_1\equiv b_1\,(\text{mod } n)$ بالفرض ، وعليه فإن $P(1)$ عبارة صحيحة . والآن لنفرض أن $P(r)$ صحيحة . إذاً $\sum_{i=1}^{r} a_i\equiv\sum_{i=1}^{r} b_i\,(\text{mod } n)$ ولإثبات صحة $P(r+1)$ ، لاحظ أن $\sum_{i=1}^{r} a_i\equiv\sum_{i=1}^{r} b_i\,(\text{mod} n)$ و $a_{r+1}\equiv b_{r+1}\,(\text{mod } n)$ بالفرض إذاً $\sum_{i=1}^{r+1} a_i=\sum_{i=1}^{r} a_i+a_{r+1}\equiv\sum_{i=1}^{r} b_i+b_{r+1}=\sum_{i=1}^{r+1} b_i\,(\text{mod} n)$ حسب مبرهنة (٣-١-٣أ) ، وعليه فإن $P(r+1)$ صحيحة ، وبالتالي فإن $P(m)$ صحيحة لكل $m\in N^*$.

نتيجة :

إذا كان $a \equiv b(\bmod n)$ وكان $m \in \mathbb{N}^*$ ، فإن $a^m \equiv b^m (\bmod n)$.

البرهان :

أفرض أن $a_i = a$ و $b = b_i$ لكل $i = 1, \cdots, m$ وطبق مبرهنة (٣-١-٥) تجد أن $a^m \equiv b^m (\bmod n)$.

□

مبرهنة ٣-١-٦ :

إذا كان $a, b \in \mathbb{Z}$ ، $n_i \in \mathbb{N}^*$ لكل $i = 1, \cdots, r$ ، وكان $m = [n_1, \cdots, n_r]$ فإن $a \equiv b \bmod (n_i)$ لكل i إذاً وإذا فقط كان $a \equiv b(\bmod m)$.

البرهان :

بما أن $a \equiv b(\bmod n_i)$ لكل $i = 1, \cdots, r$. إذاً $n_i \backslash a - b$ لكل i لكن $m = [n_1, \cdots, n_r]$. إذاً $m \backslash a - b$ ، وعليه فإن $a \equiv b(\bmod m)$.

ولإثبات العكس نفرض أن $a \equiv b(\bmod m)$. إذاً $m \backslash a - b$. لكن $n_i \backslash m$ لكل i ، إذاً $n_i \backslash a - b$ لكل i ، وعليه فإن $a \equiv b \bmod n_i$ لكل i .

□

نتيجة :

إذا كان $a, b \in \mathbb{Z}$ ، $n_i \in \mathbb{N}^*$ و $(n,r) = 1$ وكان $a \equiv b(\bmod n)$ و $a \equiv b(\bmod r)$ ، فإن $a \equiv b \bmod (nr)$.

البرهان :

بما أن $a \equiv b(\bmod n)$ و $a \equiv b(\bmod r)$ بالفرض ، إذاً $a \equiv b \bmod (m)$ ، حيث $m = [n, r]$ حسب مبرهنة (٣-١-٦) . لكن $m \cdot (n, r) = |nr|$ حسب مبرهنة (٢-٣-٥ب) و $|nr| = nr$ لأن $n, r \in \mathbb{N}^*$. إذاً $m = nr$ ، وعليه فإن $a \equiv b \bmod (nr)$.

□

والآن إلى بعض التطبيقات والأمثلة الآتية .

مثال (٤) :

أوجد باقي قسمة $1 \equiv 5^{439}$ على 3 .

الحل :

بما أن $5^2 \equiv 1(\text{mod } 3)$. إذاً $5^{438} = (5^2)^{219} \equiv 1(\text{mod } 3)$ حسب نتيجة مبرهنة (٣-١-٥) . لكن $5 \equiv 5(\text{mod } 3)$. إذاً $5^{439} \equiv 5 \ (\text{mod } 3)$ حسب مبرهنة (٣-١-٣ج) . وحيث أن $5 \equiv 2(\text{mod } 3)$. إذاً $5^{439} \equiv 2(\text{mod } 3)$ حسب مبرهنة (٣-١-٢ج) ، وعليه فإن باقي قسمة 5^{439} على 3 يساوي 2 .

مثال (٥) :

أوجد باقي قسمة $\sum_{n=1}^{100} n!$ على 15 .

الحل :

بما أن $5! \equiv 0(\text{mod } 15)$. إذاً $n! = 5!(n-5)! \equiv 0(\text{mod } 15)$ ، وعليه فإن $\sum_{n=1}^{100} n! \equiv 1!+2!+3!+4!+0 \cdots + 0(\text{mod } 15) \equiv 33 \text{ mod } 15$.

لكن $33 \equiv 3 \text{ mod} 15$. إذاً $\sum_{n=1}^{100} n! \equiv 3 \ \ (\text{mod } 15)$ ، وعليه فإن باقي قسمة $\sum_{n=1}^{100} n!$ على 15 يساوي 3 .

مثال (٦) :

أثبت أن $2^{32} + 1$ يقبل القسمة على 641 .

الإثبات :

بما أن $2^{16} \equiv 154 \ (\text{mod } 641)$ ، إذاً $2^{32} \equiv (154)^2 \ (\text{mod } 641)$ ، وعليه فإن $2^{32} + 1 \equiv (154)^2 + 1 \ (\text{mod } 641)$. لكن $(154)^2 + 1 = 23717$ و 23717 يقبل القسمة على 641 . إذاً $23717 \equiv 0 \text{ mod } 641$ ، وعليه فإن $2^{32} + 1 \equiv 0 \text{ mod } 641$ ، وبالتالي فإن $641 \setminus (2^{32} + 1)$.

مثال (٧) :

أوجد أصغر عدد صحيح m بحيث أن $33\times(37)^2+m$ يقبل القسمة على 17 .

الحل :

بمـــا أن $37\equiv 3 \pmod{17}$. إذاً $(37)^2\equiv 9 \pmod{17}$ لكـــن $33\equiv -1 \pmod{17}$. إذاً $33\times(37)^2\equiv -9 \pmod{17}$ ، وعليـــه فـــإن $\left(33\times(37)^2+9\right)$ يقبل القسمة على 17 وبالتالي فإن $m=9$.

تمـــارين

(١) إذا كان $a\equiv b \pmod{n}$ و $c>0$ ، فأثبت أن $\frac{a}{c}\equiv\frac{b}{c} \pmod{n}$.

(٢) إذا كان $a\equiv b \pmod{n}$ ، فأثبت أن $(a,n)=(b,n)$.

(٣) أوجد باقي قسمة كل من 2^{150} و 10^{38} على 7 .

(٤) أوجد باقي قسمة $1^5+2^5+\cdots+(99)^5$ على 4 .

(٥) أثبت أن $63 \setminus 2^{96}-1$ ، $97\setminus 2^{48}-1$.

(٦) بين بمثال على أن $a^2\equiv b^2 \pmod{n} \not\Rightarrow a\equiv b \pmod{n}$.

(٧) أوجد أصغر عدد صحيح موجب m بحيـــث أن $(79)^2(53)^2-m$ يقبـــل القسمة على 19 .

(٨) إذا كان n عدداً فردياً، فأثبت بالاستقراء على n أن $a^{2^n}\equiv 1 \bmod (2^{n+1})$.

(٩) (أ) إذا كان $a\equiv b \pmod{n}$ وكان $m\setminus n$ ، فأثبت أن $a\equiv b \pmod{m}$.

(ب) بـــين بمثـــال علـــى أن $a\equiv b \pmod{n}$ و $m\setminus n$ لا يعنـــي أن $a\equiv b \pmod{n}$.

(١٠) إذا كان $ab \equiv cd \pmod n$ و $b \equiv d \pmod n$ ، $(b,n)=1$ ، فأثبت أن $a \equiv c \pmod n$.

(١١) إذا كان $a \equiv b \pmod r$ و $a \equiv c \pmod s$ ، $n=(r,s)$ ، فأثبت أن $b \equiv c \pmod n$.

(١٢) أي مما يأتي عبارة صحيحة ؟ أذكر السبب .

(أ) $a \equiv 3 \bmod 5 \Rightarrow (a,5)=1$.

(ب) $a \equiv 4 \pmod 8 \Rightarrow (a,8)=4$.

(ج) $12a \equiv 15 \pmod{35} \Rightarrow 4a \equiv 5 \pmod 7$.

(د) $5a \equiv 5b \pmod 7 \Rightarrow a \equiv b \pmod 7$.

(هـ) $3a \equiv b \pmod 4 \Rightarrow 15a \equiv 5b \bmod (20)$.

(و) $12a \equiv 12b \pmod{15} \Rightarrow a \equiv b \pmod 5$.

□

٣-٢ : قابلية القسمة على 2 ، 3 ، 5 ، 7 ، 9 ، 11 ، 13

من التطبيقات المهمة للتطابقات ، إيجاد قواعد تبين ما إذا كان عدد صحيح يقبل القسمة على عدد صحيح آخر . وتعتمد تلك القواعد على تحديد العلاقة بين أرقام المقسوم المعبر عنها بالنظام العشري أو أي نظام آخر والمقسوم عليه . ولمعرفة تلك القواعد نورد ما يلي :

مبرهنة ٣-٢-١ :

إذا كان $f(x)=\sum_{i=0}^{m} c_i x^i \,,\, c_i \in \mathbb{Z}$ وكان $a \equiv b \pmod n$ ، فإن $f(a) \equiv f(b) \pmod n$.

البرهان :

بمـــا أن $a \equiv b \pmod{n}$ بـــالفرض . إذاً $a^i \equiv b^i \pmod{n}$ لكـــل $i = 0,1,\cdots,m$ حـــسب نتيجـــة مبرهنـــة (٣-١-٥) . وعليـــه فـــإن $c_i a^i \equiv c_i b^i \pmod{n}$ لكل $i = 0,1,\cdots,m$ حـــسب مبرهنـــة (٣-١-٣د) . وبالتالي فإن $\sum_{i=0}^{m} c_i a^i \equiv \sum_{i=0}^{m} c_i b^i \pmod{n}$ حسب مبرهنـــة (٣-١-٥أ) . لكـــن $f(a) \equiv \sum_{i=0}^{m} c_i a^i$ ، $f(b) = \sum_{i=0}^{m} c_i b^i$. إذاً $f(a) \equiv f(b) \pmod{n}$.

□

نتيجة :

إذا كـــــان $f(x) = \sum_{i=0}^{m} c_i x^i$, $c_i \in \mathbb{Z}$ وكـــــان $a \equiv b \pmod{n}$ و $f(a) \equiv 0 \pmod{n}$ ، فإن $f(b) \equiv 0 \pmod{n}$.

البرهان :

بمـــا أن $f(a) \equiv f(b) \pmod{n}$ حـــسب مبرهنـــة (٣-٢-١) ، و $f(a) \equiv 0 \pmod{n}$. إذاً $f(b) \equiv 0 \pmod{n}$.

□

تعريف ٣-٢-١ :

يقال عن $x = a$ أنه حل لكثيـــرة الحـــدود $f(x) = \sum_{i=0}^{n} c_i x^i \equiv 0 \pmod{n}$ ، $c_i \in \mathbb{Z}$ إذا كان $f(a) \equiv 0 \pmod{n}$.

مثال (١) :

لتكن $f(x) = 3x^2 + 2x - 5$ ، $11 \equiv 3 \pmod{8}$. إذاً $f(11) = 3(11)^2 + 2(11) - 5 = 380$ ، $f(3) = 3(9) + 2(3) - 5 = 28$ و $380 \equiv 28 \pmod{8}$. وعليه فإن $f(11) \equiv f(3) \pmod{8}$. وإذا كان $f(x) \equiv 0 \pmod{8}$ ، فإن $x = 1,5$ ، لأن $f(1) = 0 \equiv 0 \pmod{8}$ ، $f(5) = 80 \equiv 0 \pmod{8}$.

مثال (٢) :

إذا كان $a \in \mathbb{Z}$ ، فإن آحاد العدد a^2 ينتمي إلى المجموعة $\{0,1,4,5,6,9\}$.

الحل :

بما أن $10 \equiv 0 \mod 10$. إذاً $a = \sum_{i=0}^{n} a_i 10^i \equiv a_0 \pmod{10}$ حسب مبرهنة (٣-٢-١) . وعليه فإن $a^2 \equiv a_0^2 \pmod{10}$. لكن $a_0 \in \{0,1,2,3,4,5,6,7,8,9\}$. إذاً $a_0^2 \pmod{10} = 0,1,4,5,6,9$ وهذا يعني أن أحاد العدد a^2 ينتمي إلى المجموعة $\{0,1,4,5,6,9\}$.

مبرهنة ٣-٢-٢ : " قابلية القسمة على 2,3,5,9,11 "

إذا كان $a = (a_n a_{n-1} \cdots a_1 a_0)_{10}$ وكان $s = \sum_{i=0}^{n} a_i$ ، $t = \sum_{i=0}^{n} (-1)^i a_i$ ، فإن

(أ) $2 \backslash a \Leftrightarrow 2 \backslash a_0$ ، (ب) $5 \backslash a \Leftrightarrow 5 \backslash a_0$

(ج) $3 \backslash a \Leftrightarrow 3 \backslash s$ ، (د) $9 \backslash a \Leftrightarrow 9 \backslash s$

(هـ) $3 \backslash a \Leftrightarrow 11 \backslash T$

البرهان :

سنثبت (أ) ، (ج) ، (هـ) ونترك إثبات الباقي للقارئ .

لتكن $f(x) = \sum_{i=0}^{n} a_i x^i$ ، $c_i \in Z$.

(أ) بما أن $10 \equiv 0 \pmod 2$. إذاً $f(10) \equiv f(0) \pmod 2$ حسب مبرهنة (٣-٢-١) . لكن $f(10) = \sum_{i=0}^{n} a_i 10^i = a$ و $f(0) = a_0$. إذاً $a \equiv a_0 \pmod 2$ ، وعليه فإن $2 \backslash a \Leftrightarrow 2 \backslash a_0$ حسب مبرهنة (٣-١-١).

(ج) بما أن $10 \equiv 1 \pmod 3$. إذاً $f(10) \equiv f(1) \pmod 3$ حسب مبرهنة (٣-٢-١) . لكن $f(10) = a$ و $f(1) = \sum_{i=0}^{n} a_i = s$.إذاً $a \equiv s \pmod 3$ ، وعليه فإن $3 \backslash a \Leftrightarrow 3 \backslash s$ حسب مبرهنة (٣-١-١).

(هـ) بما أن $10 \equiv -1 \pmod{11}$. إذاً $f(10) \equiv f(-1) \pmod{11}$ حسب مبرهنة (٣-٢-١). لكن $f(10)=a$ و $f(-1)=t$. إذاً $a \equiv t \pmod{11}$، وعليه فإن $11 \backslash a \Leftrightarrow 11 \backslash t$.

□

مثال (٣) : أثبت أن

(أ) 147381 يقبل القسمة على 3 ، (ب) 2358792 يقبل القسمة على 9 .

(ج) 61457 يقبل القسمة على 11 .

الإثبات :

(أ) بما أن $s=1+8+3+7+4+1=24$ و $3 \backslash 24$. إذاً 147381 يقبل القسمة على 3 حسب مبرهنة (٣-٢-٢ج) .

(ب) بما أن $s=2+9+7+8+5+3+2=36$ و $9 \backslash 36$. إذاً 2358792 يقبل القسمة على 9 .

(ج) بما أن $t=\sum_{i=0}^{n} a_i = a_0 - a_1 + a_2 - a_3 + a_4$. إذاً $t=(7-5)+(4-1)+6=11$. إذاً 61457 يقبل القسمة على 11 .

مثال (٤) :

أثبت أن 874326 يقبل القسمة على 2 و 3 لكنه لا يقبل القسمة على 9 .

الإثبات :

ليكن $a=874326$ ، $a_0=6$ و 6 تقبل القسمة على 2 ، إذاً a يقبل القسمة على 2 حسب مبرهنة (٣-٢-٢أ) . وحيث أن $s=6+2+3+4+7+8=30$ و $3 \backslash s$ لكن $9 \nmid s$. إذاً $3 \backslash a$ ، بينما $9 \nmid a$ حسب مبرهنة (٣-٢-٢ج،د) .

□

مبرهنة ٣-٢-٣ : " قابلية القسمة على 7 ، 13 "

إذا كان $a=(a_n a_{n-1}\cdots a_1 a_0)_{10}$ و

$b=\frac{a-a_0}{10}=a_n 10^{n-1}+a_{n-1}10^{n-2}+\cdots a_1$ ، فإن

(أ) $7\backslash a \Leftrightarrow 7\backslash(b-2a_0)$ ، (ب) $13\backslash a \Leftrightarrow 13\backslash(b-9a_0)$

الإثبات :

(أ) بما أن $b=\frac{a-a_0}{10}$. إذاً $a=10b+a_0$ ، وعليه فإن $-2a=-20b-2a_0$. لكن $1\equiv -20 \pmod 7$. إذاً $b\equiv -20b \pmod 7$ وعليه فإن $-2a\equiv b-2a_0 \pmod 7$ ، وبالتالي فإن $7\backslash -2a \Leftrightarrow 7\backslash(b-2a_0)$. لكن $2\backslash -2a$ و $(7,-2)=1$ ، إذاً $7\backslash a$ حسب مبرهنة (٢-١-٩ب)،وعليه فإن $7\backslash a \Leftrightarrow 7\backslash(b-2a_0)$.

(ب) بما أن $a=10b+a_0$. إذاً $-9a=-90b-9a_0$. لكن $1\equiv -90 \pmod{13}$. إذاً $b\equiv -90 \pmod{13}$ ، وعليه فإن $13\backslash -9a \Leftrightarrow 13\backslash b-9a_0$. لكن $13\backslash -9a$ و $(13,-9)=1$. إذاً $13\backslash a$ حسب مبرهنة (٢-١-٩ب) ، وعليه فإن $13\backslash a \Leftrightarrow 13\backslash(b-9a_0)$.

□

مثال (٥) :

أثبت أن $7\backslash 153279$ بينما $7\nmid 65435$.

الإثبات :

بما أن $7\backslash a \Leftrightarrow 7\backslash(b-2a_0)$. إذاً

$$7\backslash 153279 \Leftrightarrow 7\backslash(15327-18) \Leftrightarrow 7\backslash 15309 \Leftrightarrow 7\backslash(1530-18)$$

$$\Leftrightarrow 7\backslash 1512 \Leftrightarrow 7\backslash(151-4) \Leftrightarrow 7\backslash 147 \Leftrightarrow 7\backslash(14-14) \Leftrightarrow 7\backslash 0$$

إذاً $7\backslash 153279$.

بما أن $(6-653)\setminus 7 \Leftrightarrow 7\setminus 6533 \Leftrightarrow 7\setminus(6543-10) \Leftrightarrow 7\setminus 65435$

$\Leftrightarrow 7\setminus 647 \Leftrightarrow 7\setminus(64-14) \Leftrightarrow 7\setminus 50 \Leftrightarrow 7\setminus 5$

و $7\nmid 5$. إذاً $7\nmid 65435$

<u>**مثال (٦) :**</u>

أثبت أن 104741 يقبل القسمة على 13 .

<u>**الإثبات :**</u>

بما أن $13\setminus a \Leftrightarrow 13\setminus(b-9a_0)$ حسب مبرهنة (٣-٢-٣ب) . إذاً

$13\setminus 104741 \Leftrightarrow 13\setminus(10474-9) \Leftrightarrow 13\setminus 10465 \Leftrightarrow 13\setminus(1046-45)$

$\Leftrightarrow 13\setminus 1001 \Leftrightarrow 13\setminus(100-9) \Leftrightarrow 13\setminus 91 \Leftrightarrow 13\setminus 0$

وعليه فإن 104741 يقبل القسمة على 13 .

<u>**ملاحظة :**</u>

يورد ابن البنا المراكشي (٦٥٤-٧٢١هـ) في مخطوطة " المقالات في علم الحساب تحقيق أحمد سليم سعيدان (١٤٧-١٤٨) " طريقتين لمعرفة ما إذا كان عدد يقبل القسمة على سبعة .

<u>**الطريقة الأولى :**</u>

تعتمد هذه الطريقة على القاعدة الآتية وهي أن " باقي قسمة عشرة على سبعة هو ثلاثة ، وباقي قسمة مائة على سبعة هو اثنان ، وباقي قسمة الألف على سبعة هو ستة ، وباقي قسمة العشرة آلاف على سبعة هو أربعة ، وباقي قسمة المائة ألف على سبعة هو خمسة ، وباقي قسمة المليون على سبعة هو واحد ، ومن ثم يعود الدور بمعنى أن باقي قسمة العشرة ملايين على سبعة هو ثلاثة وهكذا .

والعمل بهذه الطريقة هو :

" ننزل العدد في سطر ونضع تحته هذه الأعداد الواحد تحت الآحاد ، والثلاثة تحت العشرات ، والاثنين تحت المئات ، والستة تحت الآلاف ، والأربعة تحت عشرات الآلاف، والخمسة تحت مئات الألوف ، والواحد تحت الملايين ".

ثم نكرر هذه الأعداد الستة بعينها تحت باقي المراتب على التوالي ، فإذا فعلت ذلك ، فأضرب ما في كل مرتبة من العدد ، فيما تحته وأطرح الخارج ، سبعة سبعة (أقسمه على سبعة) فما بقى فأثبته على رأسها فإذا تمت المراتب بهذا العمل، فأرجع إلى الباقي فوق الخط ، فأجمع بعضه إلى بعض ، كالآحاد ، وأقسم المجتمع على سبعة فما بقى هو الجواب .

مثال (٧) : أثبت أن

(أ) 7865431 يقبل القسمة على 7 ، (ب) 65463 لا يقبل القسمة على 7 .

الإثبات :

(أ) بما أن $\frac{0532121}{\begin{array}{c}7865431\\1546231\end{array}}$ و $0+5+3+2+1+2+1=14\equiv 0 \pmod 7$.

إذاً $7 \backslash 7865431$.

(ب) بما أن $\frac{32143}{\begin{array}{c}65463\\46231\end{array}}$ و $3+2+1+4+3=13\equiv 6 \pmod 7$. إذاً $7 \nmid 65463$.

الطريقة الثانية :

إذا كان $a=(a_n\, a_{n-1}\cdots a_1\, a_0)_{10}$ ، وكان

$$[[[[3(3a_n + a_{n-1}) + a_{n-2}]\times 3 + a_{n-3}]\times 3 + \cdots]\times 3 + a_1]\times 3 + a_0$$

يقبل القسمة على 7 . فإن a يقبل القسمة على 7 .

مثال (٨) :

أثبت أن 14378 يقبل القسمة على 7 .

الإثبات :

بما أن $[[3(3\times 1+4)+3]\times 3+7]\times 3+8=245$ ولكي نثبت أن 245 يقبل القسمة على 7 ، لاحظ أن $3(3\times 2+4)+5=77$ و $7\backslash 77$. إذاً $7\backslash 245$ وعليه فإن $7\backslash 14378$.

تمـــــارين

(١) إذا كان $f(x)=x^3+2x^2-2x+1$ وكان $7\equiv 2(\text{mod }5)$ ، فأثبت أن $f(7)\equiv f(2)\ (\text{mod }5)$ ، وأوجد $a\in Z$ بحيث أن $f(a)\equiv 0(\text{mod }5)$

(٢) أثبت أن 42726132117 يقبل القسمة على 3 ، 9 .

(٣) هل أن العدد 1120378 يقبل القسمة على 2 ، 7 ، 11 ، 13 ؟

(٤) ليكن $a=(a_n\,a_{n-1}\cdots a_1\,a_0)_{10}$

(أ) إذا كان $2\backslash a$ ، فأثبت أن $a_0\in\{0,2,4,6,8\}$.

(ب) إذا كان $5\backslash a$ ، فأثبت أن $a_0\in\{0,5\}$.

(٥) إذا كـــان $a\in Z$ وكـــان أحـــاد العـــدد a^3 يـــساوي r ، فأثبـــت أن $r\in\{0,1,2,3,4,5,6,7,8,9\}$.

(٦) إذا كـــان $a\in Z$ وكـــان أحـــاد العـــدد a^4 يـــساوي r ، فأثبـــت أن $r\in\{0,1,5,6\}$.

(٧) أثبت أن كلاً من العددين 521125 ، 74833847 يقبل القسمة على 11 .

(٨) هل أن العدد 1010908899 يقبل القسمة على 7،11،13 ؟

(٩) إذا كـــان $f(a)\equiv b(\text{mod }n)$ ، فأثبـــت أن $f(a+nr)\equiv b(\text{mod }n)$ لكل $r\in Z$. " لاحظ أن $a+nr\equiv a(\text{mod }n)$ لكل $r\in Z$ " .

(١٠) إذا كـــــــان $a=(a_n\,a_{n-1}\cdots a_1\,a_0)_b$ ، $s=\sum_{i=0}^{n}a_i$ ، فأثبـــــــت أن $b-1\backslash s \Leftrightarrow b-1\backslash a$.

(١١) إذا كان $a=(a_n\,a_{n-1}\cdots a_1\,a_0)_9$ ، فأثبت $3\backslash a \Leftrightarrow 3\backslash a_0$.

(١٢) إذا كان $a=(a_n a_{n-1}\cdots a_1 a_0)_9$ ، فهل أن a يقبل القسمة على 3 ، 8 عندما :

(أ) $a=16485$ ، (ب) $a=447836$

(ج) $a=65423$ ، (د) $a=54321$

(١٣) إذا كان $a=(a_n a_{n-1}\cdots a_m a_{m-1}\cdots a_1 a_0)_{10}$ ، وكان $b=(a_{m-1} a_{m-2}\cdots a_1 a_0)_{10}$ ، فأثبت أن .

(أ) $2^m \backslash a \Leftrightarrow 2^m \backslash b$ " لاحظ أن $2^m \backslash a \Leftrightarrow a\equiv 0(\bmod 2^m)$ " .

(ب) $5^m \backslash a \Leftrightarrow 5^m \backslash b$ " لاحظ أن $5^m \backslash a \Leftrightarrow a\equiv 0(\bmod 5^m)$ " .

(ج) أوجد أعلى قوة m للعدد 2 بحيث أن 53468148 يقبل القسمة على 2^m .

(د) أوجد أعلى قوة m للعدد 5 بحيث أن 18436375 يقبل القسمة على 5^m .

(١٤) (أ) إذا كان $a=1000m+r$ ، $0\le r<1000$ وكان $b=7,11,13$ ، فأثبت أن $b\backslash a \Leftrightarrow b\backslash(m-r)$.

" ملاحظة $a=1001m-(m-r)$ "

(ب) أستخدم (أ) وأثبت أن 984211536217 يقبل القسمة على 7,13 ولا يقبل القسمة على 11 .

٣-٣ : أنظمة البواقي Residue systems

أثبتنا في مبرهنة (٣-٢-٢) أن علاقة التطابق قياس n هي علاقة تكافؤ على المجموعة $\mathbb{Z}$. وحيث أن كل علاقة تكافؤ تجزئ المجموعة المعرفة عليها إلى فصول أو صفوف تكافؤ (Equivalent classes) . إذاً

$\mathbb{Z}/\equiv_n=\{[a] \mid a\in\mathbb{Z}\}$ تجزئة للمجموعة $\mathbb{Z}$

لكن صف أو فصل التكافؤ $[a]$ والذي يحول العنصر a هو

$$\bar{a}=[a]=\{b\in Z \mid b\equiv a \bmod n\}$$
$$=\{b\in Z \mid b=a+nr\,,\, r\in Z\}=\{a\in nr \mid r\in Z\}$$

إذاً

$$\bar{0}=[0]=\{nr \mid r\in Z\}\;,\;\bar{1}=[1]=\{1+nr \mid r\in Z\}$$
$$\bar{2}=[2]=\{2+nr \mid r\in Z\}\;,\;\cdots,\;\overline{n-1}=[n-1]=\{-1+(n+1)r \mid r\in Z\}$$
$$\bar{n}=[n]=\{n+nr \mid r\in Z\}=\{(r+1)n \mid r\in Z\}=[0]$$
$$[n+1]=\{n+1+rn \mid r\in Z\}=\{1+(r+1)n \mid r\in Z\}=[1]\,,\cdots$$
$$[2n-1]=[n-1]\,,[2n]\,,[0]\;,[2n+1]=[1]\,,\cdots$$

وعليه فإذا رمزنا للمجموعة $Z/\equiv_n$ بالرمز Z_n ، نجد أن $Z_n=\{[0],[1],\cdots,[n-1]\}$ والتي تسمى مجموعة البواقي (Residue classes) قياس n ، وعندما $n=4$ ، نجد أن $Z_4=\{[0],[1],[2],[3]\}$ ، حيث

$[1]=\{\cdots,-7,-3,1,5,9,\cdots\}$ ، $[0]=\{0,\mp 4,\mp 8,\cdots\}$ ،

$[2]=\{\cdots,-6,-2,2,6,1,\cdots\},[3]=\{\cdots,-5,-1,3,7,11,\cdots\}$

والآن إلى بعض خواص فصول التطابق

مبرهنة ٣-٣-١ :

إذا كان $a,b\in Z_n$ وكان $a\neq b$ فإن $a\not\equiv b(\bmod n)$.

البرهان :

بما أن $a\neq b$ ، إذاً أما $a>b$ أو $a<b$ ، فإذا كان $a>b$ ، فإن $0\le b<a\le n-1$ ، وعليه فإن $0<a-b<n-1-b=n-(1+b)<n$ ، وبالتالي فإن $n\nmid a-b$ ، وعليه فإن $a\not\equiv b(\bmod n)$. وإذا كان $a<b$ فإن $0<b-a<n$ ، وعليه فإن $n\nmid b-a$ وهذا يعني أن $a\not\equiv b(\bmod n)$.

مبرهنة ٣-٣-٢ :

كل عدد صحيح يطابق عدداً وحيداً من الأعداد $0,1,\cdots, n-1$.

أي أن إذا كان $a\in \mathbb{Z}$ فيوجد عنصر وحيد $r\in \mathbb{Z}_n$ بحيث $a\equiv r(\bmod n)$.

البرهان :

بالقسمة الخوارزمية يمكننا إيجاد عددين وحيدين $m,r\in \mathbb{Z}$ بحيث أن $a=mn+r$ ، $0\le r<n$ ، وعليه فإن $a\equiv r(\bmod n)$ ، $r\in\{0,1,\cdots, n-1\}$ ولإثبات وحدانية r نفرض وجود عدد آخر $s\in\{0,1,\cdots, n-1\}$ و $a\equiv s(\bmod n)$. إذاً $s\equiv r$ ، وعليه فإن $s=r$ حسب مبرهنة (٣-٣-١) .

□

نستنتج من المبرهنتين (٣-٣-١) و (٣-٣-٢) أن لكل عدد صحيح موجب n يوجد n من فصول التكافؤ قياس n وهي $[0],[1],\cdots,[n-1]$ يطلق عليها البواقي قياس n (Residue classes modulo n) .

تعريف ٣-٣-١ :

يقال $\{a_0,\cdots, a_{n-1}\}$ أنها نظام بواقي تام أو مكتمل (Complete Residue system) قياس n ، إذا كان كل عدد صحيح يطابق عدداً وحيداً من الأعداد $a_0,\cdots, a_{n-1}$ قياس n .

إذاً $\{a_0,\cdots, a_{n-1}\}$ نظام بواقي تام قياس n إذا وإذا فقط كان $a\in\{[a_0],\cdots,[a_{n-1}]\}$ لكل $a\in \mathbb{Z}$.

يطلق أحياناً على المجموعة $\{[a_0],\cdots,[a_{n-1}]\}$ مجموعة البواقي التامة قياس n .

مثال (١) :

(أ) $\{0,1,\cdots, n-1\}$ نظام بواقي تام قياس n و $Z_n=\{[0],\cdots,[1]\}$ مجموعة بواقي تامة قياس n .

(ب) $c=\{0,1,2,3,4\}$ نظام بواقي تام قياس 5 ، لأن $Z_5=\{[0],[1],[2],[3],[4]\}$ مجموعة بواقي تامة قياس n .

(ج) $c=\{0,-9,12,8,14\}$ نظام بواقي تام قياس 5 ، لأن $0\equiv 0 \pmod 5$ ، $-9\equiv 1 \pmod 5$ ، $12\equiv 2 \pmod 5$ ، $8\equiv 3 \pmod 5$ ، $14\equiv 4 \pmod 5$ وبالتالي فإن $S=\{[0],[-9],[8],[12],[14]\}$ مجموعة بواقي تامة قياس 5 .

(د) $\{2,4,6,8,11\}$ نظام بواقي قياس 5 غير تام (مكتمل) ، لأن $\{[2],[4],[6],[8],[11]\}$ مجموعة بواقي غير تامة ، وذلك لأن $2\equiv 2 \pmod 5$ ، $4\equiv 4 \pmod 5$ ، $6\equiv 1 \pmod 5$ ، $8\equiv 3 \pmod 5$ ، $11\equiv 1 \pmod 5$.

<u>مبرهنة ٣-٣-٣ :</u>

$C=\{a_0,\cdots,a_{n-1}\}$ نظام بواقي تام (مكتمل) قياس n إذاً وإذا فقط كان $a_i\not\equiv a_j$ لكل $i\neq j$ ، $1\le i\ ,\ j\le n-1$.

<u>البرهان :</u>

$C=\{a_0,\cdots,a_{n-1}\}$ نظام بواقي تام (مكتمل) قياس n إذاً وإذا فقط كانت $\{[a_0],\cdots,[a_{n-1}]\}$ مجموعة بواقي تامة قياس n إذاً وإذا فقط كان $a_i\not\equiv a_j$ لكل $i\neq j$ ، $1\le i\ ,\ j\le n-1$ حسب مبرهنة (٣-٣-١) .

□

<u>نتيجة (١) :</u>

أي n من الأعداد الصحيحة المتتالية تمثل نظام بواقي تام قياس n .

<u>البرهان :</u>

ليكن a عدداً صحيحاً . إذاً $S=\{a,a+1,\cdots,a+n-1\}$ مجموعة من الأعداد الصحيحة المتتالية و $|S|=n$.

وإذا كان $a+b\,,\,a+c\in S$ ، $b,c\in C=\{0,1,\cdots,n-1\}$ ، فإن $a+b\equiv a+c \pmod n$ و $b\neq c$ يعني أن $b\equiv c \pmod n$ وهذا يناقض كون $C=\{0,1\,,\cdots,\,n-1\}$ نظام بواقي تام قياس n . إذاً $a+b\not\equiv b+c$ وعليه فإن S نظام بواقي تام قياس n حسب مبرهنة (٣-٣-٣) .

□

نتيجة (٢) :

إذا كان C نظام بواقي تام قياس n وكان $a\in Z$ ، $(a,n)=1$ ، فإن $D=\{ax+b|\,x\in C\}$ نظام بواقي تام قياس n لكل $b\in Z$.

البرهان :

نفرض أن $ax+b\equiv ay+b \pmod n$ ، $x,y\in C$. إذاً $ax\equiv ay \pmod n$ لكن $(a,n)=1$ ، إذاً $x\equiv y \pmod n$ حسب مبرهنة (٣-١-٤) ، وهذا يناقض كون $x,y\in C$ ، C نظام بواقي مكتمل قياس n . إذاً $ax+b\not\equiv ay+b$ لكل $x,y\in C$, $x\neq y$ ، وعليه فإن D نظام بواقي تام قياس n حسب مبرهنة (٣-٣-٣) .

□

مثال (٢) :

(أ) $C=\{0,1,-3,-7,17\}$ نظام بواقي تام قياس 5 ، لأن $a\not\equiv b \pmod 5$ لكل $a\neq b$ و $a,b\in C$ حسب مبرهنة (٣-٣-٣) .

(ب) $C=\{7,8,9,10,11\}$ نظام بواقي تام قياس 5 ، لأن C مجموعة من الأعداد الصحيحة المتتالية و $|C|=5$ حسب نتيجة (١) من مبرهنة (٣-٣-٣) .

(ج) $D=\{15,21,27,33,39\}$ نظام بواقي تام قياس 5 ، حسب نتيجة (٢) ، مبرهنة (٣-٣-٣) ، $C=\{0,1,2,3,4\}$ نظام بواقي تام قياس 5 و $D=\{6x+15|\,x\in C\}$.

ولدارسة أنظمة البواقي المختزلة نورد ما يلي :

تعريف ٣-٣-٢ : " دالة أويلر Euler phi function "

دالة أويلر $\phi(n)$ هي عدد الأعداد الصحيحة الموجبة الأقل من أو تساوي n والأولية نسبياً مع n .

أي أن $\phi(n)=\left|\{m\in Z \mid 1\leq m\leq n\,,\,(m,n)=1\}\right|$.

مثال (٣) :

$$\phi(3)=|\{1,2\}|=2\ ،\ \phi(4)=|\{1,3\}|=2\ ،$$
$$\phi(9)=|\{1,2,4,5,7,8\}|=6\ ،\ \phi(8)=|\{1,35,7\}|=4$$

تعريف ٣-٣-٣ :

إذا كان C نظام بواقي تام قياس n ، فيقال عن مجموعة جزئية R من C أنها نظام بواقي مختزل قياس n (Reduced residue system modulo n) ، إذا كان $R=\{a\in C \mid (a,n)=1\}$.

إذاً R نظام بواقي مختزل قياس n ، إذا كان :

(أ) $(a,n)=1$ لكل $a\in R$ ، (ب) $|R|=\phi(n)$

(ج) $a\not\equiv b(\bmod n)$ لكل $a,b\in R$ و $a\neq b$.

مثال (٤) :

(أ) إذا كان $n=6$ ، فإن $R=\{1,5\}$ نظام بواقي مختزل قياس 6 ، لأن $(1,6)=(5,6)=1$ و $|R|=\phi(6)$ ، $1\not\equiv 5(\bmod 6)$.

(ب) إذا كان $n=10$ ، فإن $R=\{1,3,7,9\}$ نظام بواقي مختزل قياس 10 ، لأن $(1,10)=(3,10)=(7,10)=(9,10)=1$ و $|R|=4=\phi(10)$ و $a\not\equiv b(\bmod 10)$ لكل $a\neq b$ ، $a,b\in R$.

(ج) $R=\{-3,-11,3,9\}$ ليس نظام بواقي مختزل قياس 10 ، لأن $9\equiv -11(\bmod 10)$.

وأخيراً إلى خواص الأنظمة المختزلة .

مبرهنة ٣-٣-٤ :

إذا كانت R نظام بواقي مختزل قياس n ، وكان $(a,n)=1$ ، فيوجد عنصر وحيد $b \in R$ بحيث أن $a \equiv b (\mathrm{mod}\ n)$.

البرهان :

ليكن C نظام بواقي تام قياس n وأن $R \subseteq C$. إذاً $(a,n)=1$ يعني وجود عنصر وحيد $b \in C$ بحيث أن $a \equiv b (\mathrm{mod}\ n)$ ، وعليه فإن $(a,n)=(b,n)$ ، لكن $(a,n)=1$. إذاً $(b,n)=1$ وبالتالي فإن $b \in R$.

□

مثال (٥) :

$R=\{1,3\}$ نظام بواقي مختزل قياس 4 ، لأن $(1,4)=(3,4)=1$ و $|R|=2=\phi(4)$ ، $1 \not\equiv 3 \bmod 4$. والآن إذا كان $a=5$ ، فإن $(a,4)=1$ و $aR=\{5,15\}$ نظام بواقي مختزل قياس 4 لأن $(5,4)=(15,4)=1$ ، $|aR|=2=\phi(4)$ ، كما أن $5 \not\equiv 15 \ (\mathrm{mod}\ 4)$.

وبصورة عامة يمكن أن نبرهن ما يلي .

مبرهنة ٣-٤-٥ :

إذا كان R نظام بواقي مختزل قياس n ، وكان $(a,n)=1$ ، فإن $aR=\{ar \mid r \in R\}$ نظام بواقي مختزل قياس n .

البرهان :

بما أن R نظام بواقي مختزل قياس n و $r \in R$ ، إذاً $(r,n)=1$. لكن $(a,n)=1$ بالفرض ، إذاً $(ar,n)=1$ حسب مبرهنة (٢-١-١٩أ) . لكن $|R|=\phi(n)$ و $|R|=|aR|$. إذاً $|aR|=\phi(n)$. والآن إذا كان $r_1, r_2 \in R$ و $a r_1 \equiv a r_2 \ (\mathrm{mod}\ n)$ ، فإن $r_1 \equiv r_2 \ (\mathrm{mod}\ n)$ حسب مبرهنة (٣-١-٤) . وهذا يناقض كون R نظام بواقي مختزل قياس n . إذاً $ar_1 \not\equiv ar_2$ لكل $ar_1, ar_2 \in aR$ ، وعليه فإن aR نظام بواقي مختزل قياس n . □

تمـــارين

(١) أثبت أن كلاً من $\{0,1,2,3,4,5\}$ ، $\{6,13,26,39,10,17\}$ نظـام بواقي تام قياس 6 .

(٢) أثبت أن كلاً من $\{-3,-2,-1,0,1,2,3,4\}$ ، $\{0,3,6,9,12,15,18,21\}$ نظام بواقي تام قياس 8 ، بينما $\{0,2,4,6,8,10,12,14\}$ نظام بواقي غير تام قياس 8 .

(٣) (أ) أثبت أن كلاً من $\{7,11,13,17,19,23,29\}$ ، $\{4,8,12,16,20,24,28\}$ ، $\{0,3,3^2,3^3,3^4,3^5,3^6\}$ ، $\{a ، a+3^{n-1} \mid a \in Z, n=1,\cdots,7\}$ نظام بواقي تام قياس 7 .

(ب) أثبت أن كلاً من $\{0,3,2^2,2^3,2^4,2^5,2^6\}$ ، $\{a ، a+2^{n-1} \mid a \in Z, n=1,2,\cdots,7\}$ نظام بواقي غير تام قياس 7 .

(٤) أي مما يأتي نظام بواقي تام قياس 9

$\{0,1,2,3,4,5,6,7,8\}$ ، $\{0,1,2,3,4,-4,-3,-2,-1\}$

$\{0,2,4,6,8,10,12,14,19\}$ ، $\{1,3,5,7,9,11,13,15,17\}$

(٥) إذا كـــان p عــــدداً أوليـــاً و $a \in Z$ ، $p \nmid a$ ، فأثبـــت أن $\{0,2a,3a,\cdots,(p-1)a\}$ نظام بواقي تام قياس p .

(٦) إذا كان $n=2m$ ، فأثبت أن $\{0,1,2,\cdots,m-1,m,-(m-1),\cdots,-2,-1\}$ نظام بواقي قياس n .

(٧) إذا كان $n=2m+1$ ، فأثبت أن $\{0,1,2,\cdots,m,-m,\cdots,-2,-1\}$ نظام بواقي تام قياس n .

(٨) أثبت أن $\{-31,-16,-8,13,25,80\}$ نظام بواقي مختزل قياس 9 .

(٩) أثبت أن $\{3,3^2,3^3,3^4,3^5,3^6\}$ نظام بواقي مختزل قياس 14 .

(١٠) إذا كان p عدداً أولياً ، فأثبت أن

$\left\{-\frac{p-1}{2},\cdots,-2,-1,1,2,\cdots,\frac{p-1}{2}\right\}$ نظام بواقي مختزل قياس p .

(١١) أثبت أن $\{4,8,12,16,20,24\}$ نظام بواقي مختزل قياس 7 .

(١٢) أي مما يأتي بنظام بواقي مختزل قياس 8 :

$\{-5,-7,5,7\}$ ، $\{11,33,55,77\}$ ، $\{3,15,21,23\}$ ، $\{-1,8,11,17\}$.

٣-٤ : التطابقات الخطية ومبرهنة الباقي الصينية .

سنركز أهتمامنا في هذا الجزء على دراسة التطابقات الخطية بمتغير واحد ومتغيريين وأنظمة التطابقات الخطية إضافة إلى مبرهنة الباقي الصينية .

تعريف ٣-٤-١ :

يقال عن علاقة تطابق أنها علاقة تطابق خطي بمتغير واحد إذا كان

$$ax \equiv b \pmod{n} \qquad \ldots(1)$$

ويقال عن $x_1 \in \mathbb{Z}$ أنه حل للتطابق الخطي (1) ، إذا كان $ax_1 \equiv b \pmod{n}$

ويقال عن حلين $x_1, x_2 \in \mathbb{Z}$ أنهما متطابقين (congruent solutions) ، إذا كان $x_1 \equiv x_2 \pmod{n}$ ، ويقال عن حلين $x_1, x_2 \in \mathbb{Z}$ أنهما غير متطابقين (incongruent solutions) ، إذا كان $x_1 \not\equiv x_2 \pmod{n}$.

مثال (١) :

(أ) إذا كان $3x \equiv 1 \pmod{4}$ ، فإن 3,7 حلان متطابقان لذلك التطابق ، لأن $3 \times 3 \equiv 1 \pmod{4}$ و $7 \times 3 \equiv 1 \pmod{4}$ ، $7 \equiv 3 \pmod{4}$.

(ب) إذا كان $2x \equiv 6 \pmod{8}$ ، فإن 7،3 حلان غير متطابقين ، لأن $2 \times 3 \equiv 6 \pmod{8}$ و $2 \times 7 \equiv 6 \pmod{8}$ بينما $7 \not\equiv 3 \pmod{8}$.

ولدراسة نوعية الحلول ، نورد الآتي :

مبرهنة ٣-٤-١ :

إذا كان $(a,n)=1$ ، فإن للتطابق الخطي $ax \equiv b \pmod{n}$ حل وحيد قياس n .

البرهان :

ليكن R نظام بواقي تام قياس n . إذاً $aR=\{ax \mid x \in R\}$ نظام بواقي تام قياس n حسب مبرهنة (٣-٣-١) ، وعليه يوجد عنصر وحيد $ax \in aR$ بحيث أن $ax \equiv b \pmod{n}$.

□

ملاحظة :

أن مبرهنة (٣-٤-١) تعني أنه إذا كان $c \in Z$ حلاً للتطابق الخطي $ax \equiv b \pmod{n}$ ، فإن $ac \equiv b \pmod{n}$ ، وأن أي عدد صحيح $e \in Z$ يكون حلاً للتطابق الخطي $ax \equiv b \pmod{n}$ إذاً وإذا فقط كان $c \equiv e \pmod{n}$ ، لأن $ac \equiv b \pmod{n}$ و $ae \equiv b \pmod{n}$ يعني أن $ac \equiv ae \pmod{n}$. لكن $(a,n)=1$ ، إذاً $c \equiv e \pmod{n}$ حسب نتيجة (٣-٣-١) .

وقبل أن نعطي نتيجتين مهمتين للمبرهنة (٣-٤-١) ، نورد التعريف الآتي .

تعريف ٣-٤-٢ :

يقال عن $b \in Z$ أنه معكوس أو نظير (Inverse) ضربي للعدد $a \in Z$ قياس n ، إذا كان $ab \equiv 1 \pmod{n}$.

مثال (٢) :

$2 \in Z$ معكوس ضربي للعدد $3 \in Z$ قياس 5 ، لأن $3 \times 2 \equiv 1 \pmod{5}$ و $4 \in Z$ معكوس ضربي للعدد $4 \in Z$ قياس 5 ، لأن $4 \times 4 \equiv 1 \pmod{5}$.

نتيجة (١) :

إذا كان p عدداً أولياً و $p \nmid a$ فإن للتطابق الخطي $ax \equiv b \pmod{n}$ حل وحيد قياس p .

البرهان :

يترك للقارئ .

نتيجة (٢) :

يكون للعدد $a \in Z$ معكوساً ضربياً قياس n إذاً وإذا فقط كان $(a,n)=1$.

البرهان :

نفرض $b \in Z$ هو المعكوس الضربي للعدد a قياس n . إذاً $ab \equiv 1 \pmod{n}$ ، وعليه فإن $n \setminus ab-1$ وهذا يعني وجود $r \in Z$ بحيث أن $ab-1=nr$ ومنا نجد أن $ab+n(-r)=1$ ، عليه فإن $(a,n)=1$ حسب مبرهنة (٢-١-٨) .

ولإثبات العكس نفرض أن $(a,n)=1$. إذاً يوجد عنصر وحيد $b \in Z$ بحيث أن $ab \equiv 1 \pmod{n}$ حسب مبرهنة (٣-٤-١) ، وعليه يوجد للعنصر $a \in Z$ معكوس ضربي قياس n .

□

مثال (٣) :

حل كلاً من التطابقات الخطية الآتية :

(أ) $4x \equiv 9 \pmod{7}$ ، (ب) $11x \equiv 25 \pmod{60}$

الحل :

(أ) بما أن $(4,7)=1$. إذاً للتطابق الخطي أعلاه حل وحيد هو $x \equiv 9 \cdot 4^{-1} \pmod{7}$. لكن $Z_7 = \{0,1,2,\cdots,6\}$ و $4^{-1}=2 \in Z_7$ لأن $4 \times 2 = 1 \in Z_7$. إذاً $x \equiv 9 \times 2 \equiv 4 \pmod{7}$.

(ب) بما أن $(11,60)=1$. إذاً للتطابق الخطي $11x \equiv 25 \pmod{60}$ حل وحيد هو $x \equiv 25 \times 11^{-1} \pmod{60}$ لكن $11^{-1} = 11 \in Z_{60}$. إذاً $x \equiv 25 \times 11 \pmod{60}$ ، ومنها نجد أن $x \equiv 25 \pmod{60}$.

مثال (٤) :

حل التطابق الخطي

$$17x \equiv 60 \bmod (94) \qquad \ldots (2)$$

الحل :

بما أن $(17,94)=1$. إذاً يوجد حل وحيد للتطابق الخطي في (2) هو $x \equiv 25 \times (17)^{-1} \bmod (94)$ وقد يكون حساب $(17)^{-1} \in Z_{94}$ صعباً لذلك يمكن حل المسألة بالطرق الآتية :

(أ) بما أن $(17,94)=1$. إذاً نوجد $r,s \in Z$ بحيث أن $94r + 17s = 1$ ، ولإيجاد r,s نستخدم القسمة الخوارزمية ، فنجد أن $94 = 5 \times 17 + 9$ ، $17 = 9 \times 1 + 8$ ، $9 = 8 \times 1 + 1$ ، $8 = 8 \times 1$ ، وعليه فإن $1 = 9 - 8$ لكن $8 = 17 - 9$. إذاً $1 = 9 - (17-9) = 2 \times 9 - 17$ لكن $9 = 94 - 5 \times 17$. إذاً $1 = 2 \times (94 - 5 \times 17) - 17 = 2 \times 94 - 11 \times 17$ ومنها نجد أن $17 \times (-11) \equiv 1 \bmod (94)$. لكن $-11 \equiv 83 \bmod (94)$. إذاً $17 \times 83 \equiv 1 \bmod (94)$ ، وعليه فإن $17^{-1} = 83 \in Z_{94}$ ، وبالتالي فإن $x \equiv 60 \times (17)^{-1} \equiv 60 \times 83 \equiv 92 \bmod (94)$ حل للتطابق (2) .

(ب) بما أن $17x \equiv 60 \bmod (94)$ و $60 \equiv -34 \bmod (94)$. إذاً $17x \equiv -34 \bmod (94)$. لكن $(17,94)=1$. إذاً $x \equiv -2 \bmod (94)$ حسب نتيجة مبرهنة (٣-١-٤) . لكن $92 \equiv -2 \bmod (94)$. إذاً $x \equiv 92 \bmod (94)$ حل للتطابق (2) .

وقبل أن نعطي طريقة أخرى لحل ذلك التطابق ، نورد ما يلي

ملاحظة: $ax \equiv b(\text{mod } n) \Leftrightarrow ax - b = ny\ ,\ y \in Z \Leftrightarrow ny \equiv -b(\text{mod } a)$

فإذا كان y_1 حلاً للتطابق الخطي $ny \equiv -b(\text{mod } a)$ فإن $ny_1 \equiv -b(\text{mod } a)$ يعني أن $ny_1 + b = ax_1$ ، $x_1 \in Z$ ، ومنها نجد أن $x_1 = \dfrac{ny_1 + 1}{a}$ حل للتطابق الخطي $ax \equiv b(\text{mod } n)$.

وبالرجوع إلى التطابق الخطي $17x \equiv 60 \text{ mod } (94)$ ، نجد أن $94y \equiv -60 \ (\text{mod } 17)$. لكن $-60 \equiv 8 \ (\text{mod } 17)$. إذاً $94y \equiv 8 \ (\text{mod } 17)$. لكن $85y \equiv 0 \ (\text{mod } 17)$. إذاً $9y \equiv 8 \ (\text{mod } 17)$ حسب مبرهنة (٣-١-٣أ) ، ومنها نجد أن $y \equiv 8(9)^{-1} \ (\text{mod } 17)$. لكن $9^{-1} = 2 \in Z_{17}$. إذاً $y \equiv 16 \ (\text{mod } 17)$ ، وعليه فإن $x = \dfrac{ny + b}{a} = \dfrac{94 \times 16 + 60}{17}$ حل للتطابق الخطي $17x \equiv 60 \ (\text{mod } 94)$

وهذا يعني أن $x \equiv 92 \ (\text{mod } 94)$ حل للتطابق الخطي $17x \equiv 60 \ (\text{mod } 94)$

والآن إلى كيفية تحديد الحلول غير المتطابقة والمبرهنة الآتية .

مبرهنة ٣-٤-٢ : ليكن $d = (a, n)$ ،

$$ax \equiv b \ (\text{mod } n) \qquad \ldots (3)$$

(أ) يوجد للتطابق الخطي (3) حل إذا وإذا فقط كان $d \setminus b$.

(ب) إذا كان $d \setminus b$ فيوجد للتطابق (3) ، d من الحلول غير المتطابقة قياس n .

البرهان :

(أ) نفرض أن x حل للتطابق الخطي (3) . إذاً $n \setminus ax - b$. لكن $d \setminus n$ و $d \setminus a$. إذاً $d \setminus b$. ولإثبات العكس لاحظ أن

$$ax \equiv b(\text{mod } n) \Leftrightarrow \frac{a}{d}x \equiv \frac{b}{d} \text{ mod } (\frac{n}{d})$$

لكن كل من a,b,n يقبل القسمة على d . إذاً $\frac{a}{d},\frac{b}{d},\frac{n}{d} \in Z$ ، وحيث أن $(\frac{a}{d},\frac{n}{d})=1$ حسب نتيجة مبرهنة (٢-١-٨) . إذاً يوجد حل وحيد للتطابق الخطي $\frac{a}{d}x \equiv \frac{b}{d} \bmod (\frac{n}{d})$ حسب مبرهنة (٣-٤-١) . وعليه يوجد حل للتطابق الخطي $ax \equiv b(\bmod n)$.

(ب) نفرض أن $\frac{b}{d}=e$ ، $\frac{n}{d}=m$ ، $\frac{a}{d}=c$. إذاً

$$ax \equiv b(\bmod n) \Leftrightarrow cx \equiv e\ (\bmod m)\ ,\ (c,m)=1$$

وعليه يوجد حل وحيد $x \equiv x_0\,(\bmod m)$ للتطابق الخطي $cx \equiv e(\bmod m)$ حسب مبرهنة (٣-٤-١) . لكن $0 \equiv mr(\bmod m)$ لكل $r \in Z$. إذاً $x \equiv x_0 + mr(\bmod m)$ حسب مبرهنة (٣-١-٣أ) ، وعليه فإن جميع الحلول المتطابقة للتطابق الخطي $cx \equiv e(\bmod m)$ على الشكل $x \equiv x_0 + mr(\bmod m)$ ، $r \in Z$. لكن ليس كل الأعداد الصحيحة على الشكل $x_0 + mr$ متطابقة قياس n . إذاً الأعداد غير المتطابقة قياس n تمثل الحلول غير المتطابقة للتطابق الخطي $ax \equiv b(\bmod n)$. فإذا كان $x_0 + rm \equiv x_0 + sm(\bmod m)$ ، فإن ذلك يعني أن $rm \equiv sm(\bmod n)$ ومنه نجد أن $r \equiv s \bmod (d)$ ، وعليه إذا كان $r \in D = \{0,1,\cdots,d-1\}$ ، فإن $(m,d)=1$ ، $R=\{mr+x_0 \mid r \in D\}$ نظام بواقي تام قياس d كما أن $|R|=d$ ، وعليه يوجد d من الحلول غير المتطابقة للتطابق الخطي (3) وهي :

$$x_0\ ,\ x_0+m\ ,\ x_0+2m,\cdots,x_0+(d-1)m$$

لكن $m=\frac{n}{d}$.

إذاً يوجد d من الحلول غير المطابقة للتطابق الخطي (3) وهي :

$$x_0\ ,\ x_0+\frac{n}{d},\cdots,x_0+\frac{(d-1)n}{d}$$

مثال (٥) :

أوجد الحلول غير المتطابقة للتطابق الخطي

$$32x \equiv 8 \pmod{42} \qquad \dots (4)$$

الحل :

بما أن $(32,42)=2$ و $2 \backslash 8$. إذاً يوجد حلان غير متطابقين للتطابق الخطي (4) حسب مبرهنة (٣-٤-٢) . لكن

$32x \equiv 8 \pmod{42} \Rightarrow 16x \equiv 4 \pmod{21} \quad \cdots \quad (5)$. وحيث أن $(16,21)=1$. إذاً يوجد حل للتطابق الخطي (5) هو $x \equiv 4(16)^{-1} \pmod{21}$ لكن $16^{-1}=4 \in Z_{21}$. إذاً $x_0 \equiv 16 \pmod{21}$ ، لكن $D=\{0,1\}$ نظام بواقي تام قياس 2 . إذاً $R=\{x_0+21r \mid e \in D\}$ تمثل مجموعة الحلول غير المتطابقة للتطابق الخطي (4) ومنها نجد أن $x=16\,,\,37$ حلان غير متطابقتين الخطي (4) .

مثال (٦) :

إذا كان $5x \equiv 8 \pmod{15}$ ، فإن $(5,15)=3$ و $3 \nmid 8$. إذاً لا يوجد حل للتطابق الحظي $5x \equiv 8 \pmod{15}$.

مثال (٧) :

حل التطابق الخطي

$$6x \equiv 9 \pmod{21} \qquad \dots (6)$$

الحل :

بما أن $(6,21)=3$ و $3 \backslash 9$. إذاً يوجد ثلاثة حلول غير متطابقة للتطابق الخطي (6) ، ولإيجادها لاحظ أن

$$6x \equiv 9 \pmod{21} \Leftrightarrow 2x \equiv 3 \pmod{7} \qquad \dots (7)$$

وعليه فإن $x_0 \equiv 3(2^{-1}) \pmod{7}$. لكن $2^{-1}=4 \in Z_7$.

إذاً $x_0 = 3(4) \equiv 5 (\bmod 7)$ وحيث أن $D = \{0, 1, 2\}$ و $R = \{7r + x_0 | r \in D\} = \{5 + 7r | r \in D\}$. إذاً $R = \{5, 12, 19\}$ ، وعليه فإن الحلول غير المتطابقة للتطابق الخطي (6) هي 5,12,19 .

مثال (٨) :

حل التطابق

$$15x \equiv 25 \ (\bmod 35) \qquad \dots (8)$$

الحل :

بما أن $(15,35) = 5$ و $5 \backslash 25$. إذاً يوجد خمسة حلول غير متطابقة للتطابق الخطي (8) ، ولإيجاد تلك الحلول ، لاحظ أن

$$15x \equiv 25 \ (\bmod 35) \Leftrightarrow 3x \equiv 5 \ (\bmod 7) \qquad \dots (9)$$

لكن $(3,7) = 1$. إذاً $3^{-1} = 5 \in Z_7$ ، وعليه فإن $x_0 \equiv 3^{-1}(5) \equiv 4 (\bmod 7)$ لكن $D = \{0,1,2,3,4\}$ نظام بواقي تام قياس 5 ، إذاً $R = \{4 + 7r | r \in D\} = \{4,11,18,25,32\}$ هي مجموعة الحلول غير المتطابقة للتطابق (8) .

والآن إلى المبرهنة الآتية .

مبرهنة ٣-٤-٣ :

إذا كان $a_1, a_2, n, r \in Z$ ، $n, r > 0$ ، فيوجد حل لنظام التطابق الخطي

$$x \equiv a_1 \ (\bmod n) \ ، \qquad \dots (10)$$

$$x \equiv a_2 \ (\bmod r) \qquad \dots (11)$$

إذاً وإذا فقط كان $(n,r) \backslash (a_2 - a_1)$.

وإذا كان x حلاً للنظام أعلاه فإن $x \equiv x_1 \ (\bmod m)$ ، حيث $m = [n,r]$.

البرهان :

بما ن $x \equiv a_1 \ (\bmod n)$. إذاً يوجد $s \in Z$ بحيث أن $x = a_1 + ns$ ، وبالتعويض في (11) ينتج أن $a_1 + ns \equiv a_2 \ (\bmod r)$ ، ومنها نجد أن

$$ns \equiv a_2 - a_1 \ (\bmod r) \qquad \dots (12)$$

إذاً يوجد حل للتطابق الخطي (12) إذا وإذا فقط كان $(n,r)\setminus a_2 - a_1$ حسب مبرهنة (٣-٤-٢) . والآن لنفرض أن x_0 حل للتطابق الخطي (12) . إذاً جميع الحلول غير المتطابقة للتطابق الخطي (12) على الشكل $s = x_0 + \frac{tr}{(n,r)}$ ، $t \in Z$ حسب مبرهنة (٣-٤-٢) ، ومنها نجد أن

$$x = a_1 + ns = a_1 + (x_0 + \frac{rt}{(n,r)})n = a_1 + x_0 n + \frac{nrt}{(n,r)}$$

لكن $x_1 = a_1 + x_0 n \in Z$ و $\frac{nr}{(n,r)} = m$ حسب مبرهنة (٢-٣-٥) . إذاً $x = x_1 + mt$ ، وعليه فإن $x \equiv x_1 (\text{mod } m)$.

□

مثال (٩) :

... (13) $x \equiv 3 \ (\text{mod } 6)$ ،

... (14) $x \equiv 9 \ (\text{mod } 15)$

الحل :

بما أن $(6,15) = 3$ و $3 \setminus (9-3)$. إذاً يوجد حل للنظام المعطي ، ولإيجاد ذلك الحل ، لاحظ أن

... (15) $x = 3 + 6r$ ، $r \in Z$

وبالتعويض في (14) ينتج أن $3 + 6r \equiv 9 (\text{mod } 15)$ ومنها نجد أن $6r \equiv 6 \ (\text{mod } 15)$ ، وعليه فإن $r \equiv 1 \text{ mod } (\frac{15}{(6,15)})$ ، وهذا يعني أن

$r \equiv 1 \ (\text{mod } 5)$ ، وعليه فإن

... (16) $r = 1 + 5t$ ، $t \in Z$

ومن (16) ، (15) ينتج أن $x = 3 + 6(1+5t) = 9 + 30t$ ، $t \in Z$ ، وعليه فإن $x \equiv 9 (\text{mod } 30)$.

والآن إلى مبرهنة الباقي الصينية والتي سُميتْ بهذا الاسم لأن الرياضي الصيني Sun – Tsu سأل في القرن الأول قبل الميلاد عن العدد الذي إذا قُسم على 3 كان الباقي 2 ، وإذا قسم على 5 كان الباقي 3 ، وإذا قسم على 7 كان الباقي 2 ، وهذه المسألة تكافئ إيجاد الحل لنظام التطابق $x \equiv 2 \pmod 3$ ، $x \equiv 3 \pmod 5$ ، $x \equiv 2 \pmod 7$.

مبرهنة ٣-٤-٤ : " مبرهنة الباقي الصينية Chinese Remainder Theorom "

إذا كان $n_1, n_2, \cdots, n_r$ أعداداً صحيحة موجبة وكان $(n_i, n_j) = 1$ لكل $i \neq j$، فيوجد للنظام

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

حل وحيد قياس $n = \prod_{i=1}^{r} n_i$

البرهان : " بالأستقراء على r "

فإذا كان $r = 1$ فلا يوجد ما نبرهنه ، أما إذا كان $r = 2$ فإن $x \equiv a_1 \pmod{n_1}$، $x \equiv a_2 \pmod{n_2}$ و $(n_1, n_2) = 1$. ومبرهنة (٣-٤-٣) تضمن وجود حل وحيد لذلك النظام قياس $n_1 n_2$ وعليه فإن المبرهنة صحيحة عندما $r = 2$.

والآن أفرض أن المبرهنة صحيحة إلى $(r-1)$ من المعادلات ، تجد وجود حل وحيد $x \equiv c \bmod (\prod_{i=1}^{r-1} n_i)$. ولإثبات صحة المبرهنة إلى r من المعادلات، لاحظ أن $x \equiv c \bmod (\prod_{i=1}^{r-1} n_i)$ و $x \equiv a_r \pmod{n_r}$. لكن $(\prod_{i=1}^{r-1} n_i , n_r) = 1$. إذاً يوجد حل وحيد قياس $n = \prod_{i=1}^{r-1} n_i$ حسب مبرهنة (٣-٤-٣) .

مثال (١٠) :

حل النظام

$$\left.\begin{array}{ll} x \equiv 2 \pmod 3 & \cdots (17) \\ x \equiv 3 \pmod 5 & \cdots (18) \\ x \equiv 2 \pmod 7 & \cdots (19) \end{array}\right\} \quad \cdots (I)$$

الحل :

بما أن $(3,5) = (5,7) = (3,7) = 1$. إذاً يوجد للنظام (I) حل وحيد قياس $(3 \times 5 \times 7 = 105)$ ، حسب مبرهنة الباقي الصينية . ولإيجاد ذلك الحل ، لاحظ أن

$$x \equiv 2 \pmod 3 \Rightarrow x = 2 + 3r \ , \ r \in Z \quad \ldots (20)$$

وبالتعويض في (18) ينتج أن $2 + 3r \equiv 3 \pmod 5$ ، ومنها نجد أن $3r \equiv 1 \pmod 5$ ، وعليه فإن $r = 3^{-1} = 2 \in Z_5$ ، وبالتالي فإن $r \equiv 2 \pmod 5$ ، وعليه فإن $r = 2 + 5t$ ، $t \in Z$ ، وبالتعويض في (20) ينتج أن

$$x = 8 + 15t \quad \ldots (21)$$

ومن (19) ، (21) نجد أن

$$8 + 15t \equiv 2 \pmod 7 \Rightarrow 15t \equiv -6 \pmod 7$$
$$\Rightarrow 5t \equiv -2 \equiv 5 \pmod 7 \Rightarrow t \equiv 1 \pmod 7$$

وعليه فإن $t = 1 + 7m$ ، $m \in Z$ ، وبالتعويض في (21) ينتج أن

$$x = 23 + 105m \Rightarrow x \equiv 23 \bmod (105)$$

مثال (١١) :

أوجد أصغر عدد صحيح موجب إذا قُسم على 2 كان الباقي 3 ، وإذا قُسم على 5 كان الباقي 2 ، وإذا قُسم على 3 كان الباقي 5 ، وإذا قُسم على 7 كان الباقي 11 .

الحل :

بما أن

$$x \equiv 3 \pmod 2 \qquad \dots (22)$$
$$x \equiv 2 \pmod 5 \qquad \dots (23)$$
$$x \equiv 5 \pmod 3 \qquad \dots (24)$$
$$x \equiv 11 \pmod 7 \qquad \dots (25)$$

و $1 = (2,7) = (3,7) = (5,7) = (5,3) = (2,5) = (2,3) = (2,5)$ ، إذاً يوجـــد حل وحيد للنظام أعلاه $x \equiv x_1 \bmod (210)$ ، ولإيجاد ذلك الحل ، لاحظ أن

$$x \equiv 3 \pmod 2 \Rightarrow \exists r \in \mathbb{Z} : x = 3 + 2r \qquad \dots (26)$$

وبالتعويض في (23) ينتج أن

$$3 + 2r \equiv 2 \pmod 5 \Rightarrow 2r \equiv -1 \pmod 5 \Rightarrow r \equiv 2 \pmod 5$$
$$\Rightarrow \exists t \in \mathbb{Z} : \quad r = 2 + 5t \qquad \dots (26)$$

ومن (27) ، (26) ينتج أن

$$x = 7 + 10t \qquad \dots (28)$$

ومن (28) ، (24) ينتج أن

$$7 + 10t \equiv 5 \pmod 3 \Rightarrow 10t \equiv -2 \pmod 3 \Rightarrow 10t \equiv 1 \pmod 3$$
$$\Rightarrow t \equiv 1 \pmod 3 \Rightarrow \exists s \in \mathbb{Z} : \quad t = 1 + 3s$$

وبالتعويض في (28) ينتج أن

$$x = 17 + 30s \qquad \dots (29)$$

ومن (29) ، (25) ينتج أن

$$17 + 30s \equiv 11 \pmod 7 \Rightarrow 30s \equiv 1 \pmod 7 \Rightarrow 2s \equiv 1 \pmod 7$$
$$\Rightarrow s \equiv 2^{-1} = 4 \in \mathbb{Z}_7$$

وعليـــه فـــإن $s = 4 + 7n$ ، $n \in \mathbb{Z}$ ، وبـــالتعويض فـــي (29) ينـــتج أن $x = 137 + 210n$ ، وعليه فـــإن $x \equiv 137 \pmod{210}$. إذاً أصـــغر عـــدد صحيح موجب يحقق المطلوب هو 137 .

مثال (١٢) :

حل التطابق الخطي $13x \equiv 17 \pmod{42}$

الحل :

لاحظ أن

$$13x \equiv 17 \pmod{2} \Leftrightarrow x \equiv 1 \pmod{2} \qquad \ldots (30)$$

$$13x \equiv 17 \pmod{42} \Leftrightarrow 13x \equiv 17 \pmod{3} \Leftrightarrow x \equiv 2 \pmod{3} \qquad \ldots (31)$$

$$13x \equiv 17 \pmod{7} \Leftrightarrow x \equiv 4 \pmod{7} \qquad \ldots (32)$$

لأن

$$13x \equiv 17 \pmod{7} \Leftrightarrow 13x \equiv 3 \pmod{7} \Leftrightarrow 14x \equiv x + 3 \pmod{7}$$

$$\Leftrightarrow 0 \equiv x + 3 \pmod{7} \Leftrightarrow x \equiv -3 \pmod{7} \Leftrightarrow x \equiv 4 \pmod{7}$$

وحيث أن $(2,3) = (2,7) = (3,7) = 1$. إذاً للنظام أعلاه حل وحيد حسب مبرهنة الباقي الصينية ، ولإيجاد ذلك الحل ، لاحظ أن

$$x = 1 + 2r \text{ ، } r \in \mathbb{Z} \qquad \ldots (33)$$

ومن (31) ، (33) ينتج أن

$$r \equiv 2 \pmod{3} \Rightarrow r = 2 + 3t \ , \ t \in \mathbb{Z}$$

وبالتعويض في (33) ، نجد أن

$$x = 5 + 6t \qquad \ldots (34)$$

ومن (34) ، (32) ، نجد أن

$$t \equiv 1 \pmod{7} \Rightarrow t = 1 + 7n \ , \ n \in \mathbb{Z}$$

وبالتعويض في (34) ينتج أن $x = 11 + 42n$ ، وعليه فإن $x \equiv 11 \pmod{42}$.

وأخيراً إلى دراسة التطابق الخطي بمتغيرين والمبرهنة الآتية .

مبرهنة ٣-٤-٥ : يكون للتطابق الخطي

$$ax + by \equiv c \pmod{n} \qquad \ldots (35)$$

حلاً إذاً وإذا فقط كان $d \backslash c$ حيث $d = (a,b,n)$.

البرهان :

بما أن $ax + by \equiv c \pmod{n} \Leftrightarrow by \equiv c - ax \pmod{n}$. إذاً يوجد حل للتطابق الخطي (35) ، إذاً وإذا فقط كان $(b,n) \backslash (c - ax)$ حسب مبرهنة (٣-٤-٢) . لكن

$$(b,n) \backslash (c - ax) \Leftrightarrow ax \equiv c \bmod (b,n) \qquad \dots (36)$$

وبتطبيق مبرهنة (٣-٤-٢) مرة أخرى نجد أن للتطابق (36) حل إذاً وإذا فقط كان $(a,(b,n)) \backslash c$. لكن $(a,(b,n)) = (a,b,n) = d$. إذاً للتطابق الخطي (35) حل إذاً وإذا فقط كان $d \backslash c$.

□

مثال (١٣) :

حل التطابق الخطي

$$5x + 7y \equiv 11 \pmod{9} \qquad \dots (37)$$

الحل :

بما أن $(5,7,9) = 1$. إذاً يوجد حل للتطابق الخطي (37) حسب مبرهنة (٣-٤-٥) . ولإيجاد ذلك الحل ، لاحظ أن $5x \equiv 11 - 7y \pmod{9} \equiv 2 + 2y \pmod{9}$. لكن $18 + 18y \equiv 0 \pmod{9}$ إذاً $5x \equiv 2 + 2y + 18 + 18y \pmod{9}$ ، وعليه فإن $5x \equiv 20 + 20y \pmod{9}$ لكن $(5,9) = 1$. إذاً $x \equiv 4 + 4y \pmod{9}$. لكن أي قيمة من قيم $y \in Z_9$ تعطي قيمة إلى $x \in Z_9$. إذاً مجموعة الحلول غير المتطابقة للتطابق الخطي (37) هي

$$\begin{aligned} s &= \{ (4 + 4y , y) \mid y \in Z_9 \} \\ &= \{(4,0) , (8,1) , (3,2) , (7,3) , (2,4) , (6,5) , (1,6) , (7,7) ,(0,8)\} \end{aligned}$$

□

تمـــــارين

(١) أوجد مجموعة الحل لكل من التطابقات الخطية الآتية :

(أ) $3x \equiv 4 \pmod{5}$ ، (ب) $8x \equiv 3 \pmod{27}$

(ج) $20x \equiv 30 \pmod{4}$ ، (د) $64x \equiv 83 \pmod{105}$

(هـ) $15x \equiv 24 \pmod{35}$ ، (و) $14x \equiv 18 \pmod{24}$

(٢) حل كلاً من الأنظمة الآتية :

(أ) $x \equiv 4 \pmod{6}$, $x \equiv 13 \pmod{15}$ ، (ب) $x \equiv 8 \pmod{9}$, $x \equiv 2 \pmod{3}$

(ج) $x \equiv 7 \pmod{21}$, $x \equiv 3 \pmod{8}$ ، (د) $x \equiv 2 \pmod{15}$, $x \equiv 7 \pmod{16}$

(٣) حل كلاً من الأنظمة الآتية :

(أ) $x \equiv 1 \pmod{11}$, $x \equiv 1 \pmod{6}$, $x \equiv 3 \pmod{7}$ ، (ب) $x \equiv 2 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$

(ج) $x \equiv 7 \pmod{9}$, $x \equiv 10 \pmod{4}$, $x \equiv 1 \pmod{7}$ ، (د) $x \equiv 3 \pmod{10}$, $x \equiv 11 \pmod{13}$, $x \equiv 15 \pmod{17}$

(هـ) $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$, $x \equiv 4 \pmod{9}$, $x \equiv 5 \pmod{11}$ ، (و) $2x \equiv 1 \pmod{5}$, $3x \equiv 9 \pmod{6}$, $4x \equiv 1 \pmod{7}$, $5x \equiv 9 \pmod{11}$

(٤) أوجد أصغر عدد صحيح إذا قُسم على 3 كان الباقي 1 ، وإذا قُسم على 4 كان الباقي 2 ، وإذا قسم على 5 كان الباقي 3 .

(٥) بإستخدام مبرهنة الباقي الصينية ، أوجد حل كل من التطابقات الخطية الآتية

(أ) $7x \equiv 1 \pmod{180}$ ، (ب) $8x \equiv 7 \pmod{165}$

(٦) برهن على وجود حل للنظام :

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

إذاً وإذا فقط كان $(n_i, n_j) \setminus (a_i - a_j)$ لكل i،j حيث $1 \le i < j \le r$ ، ثم أثبت أنه إذا كان ذلك الحل موجوداً فإنه على الشكل $x \equiv x_1 \pmod{m}$ حيث $m = [n_1, \cdots, n_r]$.

(٧) حل كلاً مما يأتي :

(أ) $x \equiv 8 \pmod{9}$ ، $x \equiv 2 \pmod{3}$ ، $x \equiv 5 \pmod{7}$

(ب) $x \equiv 4 \pmod{6}$ ، $x \equiv 13 \pmod{15}$ ، $x \equiv 8 \pmod{14}$ ، $x \equiv 1 \pmod{7}$

٣-٥ : " مبرهنتي أويلر وفيرما Euler and Fermat Theorens "

يعرف الصينيون قبل أكثر من 2000 سنة بأن $(2^p - 2)$ يقبل القسمة على p لأي عدد أولي p ، وقد عمم فيرما تلك الحقيقة بدون إثبات عام ١٦٤٠م إلى ما يسمى مبرهنة فيرما الصغيرة "Fermat's Little Theorem" والتي تنص على أن " **إذا كان a عدداً صحيحاً لا يقبل القسمة على العدد الأولي p ، فإن $(a^{p-1} - 1)$ يقبل القسمة على p** " .

وقد حصل الألماني ليبنز (١٦٤٦-١٧١٦) على نفس النتيجة وأثبتها بالأستقراء الرياضي سنة ١٦٨٣م "ولم ينشر البرهان". أما أول إثبات منشور لتلك المبرهنة فقد كان لأويلر سنة ١٧٣٦م ، ثم عمم أويلر تلك المبرهنة سنة ١٧٦٠م .

وسنركز أهتمامنا في هذا الجزء على دراسة تلك المبرهنتين وبعض تطبيقاتهما .

مبرهنة ٣-٥-١ : " Euler's Theorem "

إذا كان n عدداً صحيحاً موجباً وكان $a \in Z$ ، $(a,n)=1$ فإن $a^{\phi(n)} \equiv 1 \pmod n$.

البرهان :

ليكن $R=\{r_1,\cdots,r_{\phi(n)}\}$ نظام بواقي مختزل قياس n . إذاً $aR=\{ar_1,\cdots,ar_{\phi(n)}\}$ نظام بواقي مختزل قياس n حسب مبرهنة (٣-٣-٥) ، كما أن $|R|=|aR|=\phi(n)$. وعليه فإن كل عنصر من عناصر aR يطابق عنصراً وحيداً من عناصر R ، وبالتالي فإن

$$\prod_{i=1}^{\phi(n)}(a\,r_i) \equiv \prod_{i=1}^{\phi(n)} r_i \pmod n$$ ، وعليه فإن

$$a^{\phi(n)} \cdot \prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} r_i \pmod n$$. لكن

$(r_i,n)=1$ لكل $1 \le i \le \phi(n)$. إذاً $(\prod_{i=1}^{\phi(n)} r_i, n)=1$ حسب مبرهنة (٢-١-٩أ) ، وعليه فإن $a^{\phi(n)} \equiv 1 \pmod n$ حسب نتيجة مبرهنة (٣-١-٤) .

□

نتيجة (١) : " مبرهنة فيرما الصغرى Fermat's Little Theorem "

إذا كان p عدداً أولياً وكان $a \in Z$ و $p \nmid a$ ، فإن $a^{p-1} \equiv 1 \pmod p$.

البرهان :

بما أن $p \nmid a$. إذاً $(a,p)=1$ ، وعليه فـإن $a^{\phi(p)} \equiv 1 \pmod p$ حسب مبرهنة أويلر . لكن

$$\phi(p)=\left|\left\{m \in Z \middle| 1 \le m \le p : (m,p)=1\right\}\right| = \left|\{1,2,3,\cdots,p-1\}\right|$$
$$=p-1$$

إذاً $a^{p-1} \equiv 1 \pmod p$.

□

نتيجة (٢) :

إذا كان p عدداً أولياً فإن $a^p \equiv a \pmod p$.

البرهان :

أما $p \setminus a$ أو $p \nmid a$. إذا كان $p \setminus a$ فإن $a \equiv 0 \pmod p$ ، وعليـه فـإن $a^p \equiv 0 \pmod p$ حسب نتيجة مبرهنة (٣-١-٥) . وبالتالي فإن $a^p \equiv a$.
أما إذا كان $p \nmid a$ ، فإن $a^{p-1} \equiv 1 \pmod p$ حسب مبرهنة فيرما ، ومنها نجـد أن $a^p \equiv a \pmod p$ حسب مبرهنة (٣-١-٣د) .

□

نتيجة (٣) :

إذا كان $(a,n)=1$ ، فإن $a^{\phi(n)-1}$ معكوس ضربي للعدد الصحيح a قياس n .

البرهان :

بمـــــا أن $(a,n)=1$. إذاً $a^{\phi(n)} \equiv 1 \pmod n$ ، وعليـــــه فـــــإن $a \cdot a^{\phi(n)-1} \equiv 1 \pmod n$ ، ومنها نجد أن $a^{\phi(n)-1}$ معكوس ضـــربي للعـــدد a قياس n .

□

نتيجة (٤) :

إذا كان $(a,n)=1$ ، فـــإن الحـــل الوحيـــد للتطـــابق $ax \equiv b \pmod n$ هـــو $x \equiv a^{\phi(n)-1} b \pmod n$.

البرهان :

بما أن $(a,n)=1$. إذاً الحل الوحيد للتطابق الخطي $ax \equiv b \pmod{n}$ هو $x \equiv a^{-1} b \pmod{n}$ حسب مبرهنة (٣-٤-١) . لكن $a^{-1} = a^{\phi(n)-1}$ حسب نتيجة (٣) . إذاً الحل الوحيد هو $x \equiv a^{\phi(n)-1} \cdot b \pmod{n}$.

□

نتيجة (٥) :

إذا كان $(a,n) = (a-1\,,\,n) = 1$ ، فإن

$$1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \pmod{n} .$$

البرهان :

بما أن $(a,n)=1$. إذاً $a^{\phi(n)} \equiv 1 \pmod{n}$ حسب مبرهنة أويلر . لكن $a^{\phi(n)} - 1 = (a-1)(a^{\phi(n)-1} + \cdots + a^2 + a + 1)$ و $a^{\phi(n)} - 1 \equiv 0 \pmod{n}$ إذاً $(a-1)(a^{\phi(n)-1} + \cdots + a^2 + a + 1) \equiv 0 \pmod{n}$. لكن $(a-1\,,\,n)=1$ إذاً $(a^{\phi(n)-1} + \cdots + a^2 + a + 1) \equiv 0 \pmod{n}$ حسب نتيجة مبرهنة (٣-١-٤) .

□

ملاحظة :

عكس مبرهنة فيرما ليس صحيحاً . أي أنه إذا كان $(a,p)=1$ $a^{p-1} \equiv 1 \pmod{p}$ فقد لا يكون p عدداً أولياً كما يوضح ذلك المثال الآتي :
$5^3 \equiv 1 \pmod{4}$ و $(5,4)=1$ بينما 4 ليس أولياً .

والآن إلى بعض التطبيقات والمبرهنة الآتية .

مبرهنة ٣-٥-٢ :

إذا كان p,q عددين أوليين مختلفين وكان $a^p \equiv a \pmod{q}$ ، $a^q \equiv a \pmod{p}$ ، فإن $a^{pq} \equiv a \pmod{pq}$.

البرهان :

بما أن $(a^q)^p \equiv a^q \pmod p$ حسب نتيجة (٢) من مبرهنة أويلر ، وبما أن $a^q \equiv a \pmod p$ بالفرض . إذاً $a^{pq} \equiv a \pmod p$.

وبنفس الطريقة يمكن أن نبرهن على أن $a^{pq} \equiv a \pmod q$. إذاً $a^{pq} \equiv a \pmod{pq}$ حسب نتيجة (٢) مبرهنة (٢-١-٨) .

□

والآن إلى الأمثلة الآتية

مثال (١) :

أثبت أن $a^{37} \equiv a \pmod{1729}$.

الإثبات :

بما أن $1729 = 7 \times 13 \times 19$. إذاً إذا كان $(a,7) = (a,13) = (a,19) = 1$ ، فإن $a^6 \equiv 1 \pmod 7 , a^{12} \equiv 1 \pmod{13}$ ، $a^{18} \equiv 1 \pmod{19}$ حسب مبرهنة فيرما . وعليه فإن $a^6 \cdot a^{12} \cdot a^{18} \equiv 1 \bmod (1729)$ وهذا يعني أن $a^{36} \equiv a \bmod (1729)$ حسب مبرهنة (٣-١-٦) ، إذاً $a^{37} \equiv a \bmod (1729)$ حسب مبرهنة (٣-١-٣د) .

مثال (٢) :

أوجد المعكوس الضربي للعدد 5 قياس 8 .

الحل :

بما أن $(5,8) = 1$. إذاً $5^{-1} = 5^{\phi(8)-1}$. لكن $\phi(8) = 4$. إذاً $5^{-1} = 5^3 = 125$ لكن $125 \equiv 5 \pmod 8$. إذاً $5^{-1} (\text{mod }) = 5$.

مثال (٣) :

حل التطابق الخطي $3x \equiv 5 \pmod 8$.

الحل :

بمـــا أن $(3,8)=1$. إذاً الحـــل والوحيـــد للتطـــابق $3x \equiv 5 \pmod 8$ هـــو $x \equiv 3^{\phi(8)-1} \cdot 5 \pmod 8$. لكن $\phi(8)=4$. إذاً $x \equiv 3^3 \cdot 5 \bmod 8$. لكـــن $3^3 \cdot 5 = 135 \equiv 7 \pmod 8$. إذاً $x \equiv 7 \pmod 8$ حل للتطابق المعطى .

مثال (٤) :

أوجد باقي قسمة 3^{439} على 5 .

الحل :

بما أن $(3,5)=1$. إذاً $3^4 \equiv 1 \pmod 5$ حسب مبرهنة فيرما ، وعليـــه فـــإن $(3^4)^{109} = 3^{436} \equiv 1 \pmod 5$ ، ومنها نجد أن $3^{436} \times 3^3 \equiv 3^3 \times 1 \pmod 5$ حسب مبرهنة (٣-١-٣د) . إذً $3^{439} \equiv 27 \pmod 5$. لكن $27 \equiv 2 \pmod 5$ إذاً $3^{439} \equiv 2 \pmod 5$ ، وعليه فإن باقي قسمة 3^{439} على 5 يساوي 2 .

مثال (٥) :

أوجد باقي قسمة $(1234)^{8765434}$ على 11 .

الحل :

بمـــا أن $1234 \equiv (4-3)+(2-1) = 2 \pmod{11}$ حـــسب مبرهنـــة (٣-٢-٢هـ) . إذاً

$$(1234)^{8765434} \equiv 2^{8765434} \pmod{11} \qquad \dots (1)$$

لكن . $(2,11)=1$. إذاً $2^{10} \equiv 1 \pmod{11}$ حـــسب مبرهنـــة فيرمـــا . لكـــن $8765434 = 876543 \times 10 + 4$. إذاً $2^{8765434} = 2^{876543 \times 10} \cdot 2^4 = (2^{10})^{876543} \cdot 2^4$ ، وعليـــــه فـــــإن $2^{8765434} \equiv 1(2^4) \pmod{11}$. لكن $2^4 \equiv 5 \pmod{11}$. إذاً

$$2^{8765434} \equiv 5 \pmod{11} \qquad \dots (2)$$

ومن (1) ، (2) ينتج أن $(1234)^{8765434} \equiv 5 \pmod{11}$ ، وعليه فـــإن بـــاقي القسمة يساوي 5 .

مثال (٦) :

أوجد مرتبي الآحاد والعشرات للعدد $(23)^{442}$.

الحل :

لإيجاد مرتبي الآحاد والعشرات نوجد باقي قسمة العدد على 100 ، ولإيجاد ذلك ، لاحظ أن $(100,23)=1$ ، $\phi(100)=40$. إذاً $(23)^{40}\equiv 1 \pmod{100}$ حسب مبرهنة أويلر . وعليه فإن $(23)^{40\times 11}\equiv 1 \pmod{100}$ وهذا يعني أن $(23)^{440}\equiv 1 \pmod{100}$. إذاً $(23)^{440}\times(23)^2\equiv(23)^2 \pmod{100}$ حسب مبرهنة (٣-١-٣د) ، وعليه فإن $(23)^{442}\equiv(23)^2 \pmod{100}$. لكن $(23)^2=529\equiv 29 \pmod{100}$. إذاً $(23)^{442}\equiv 29 \pmod{100}$ ، وعليه فإن مرتبي الآحاد والعشرات هما 9 ، 2 على التوالي .

والآن إلى المبرهنة الآتية التي توضح الشوط التي يجب توفرها ليكون عكس مبرهنة فيرما صحيحاً .

مبرهنة ٣-٥-٣ : " عكس مبرهنة فيرما "

إذا كان $n\geq 2$ وكان $a^{n-1}\equiv 1 \pmod{n}$ لكل $1\leq a\leq n-1$ ، فإن n عدد أولي .

البرهان :

بما أن $a^{n-1}\equiv 1 \pmod{n}$ لكل $1\leq a\leq n-1$. إذاً $a^{n-2}\cdot a\equiv 1 \pmod{n}$ لكل $1\leq a\leq n-1$ ، وعليه فإن للعنصر a معكوس ضربي هو a^{n-2} ، وبالتالي فإن $(a,n)=1$ لكل $1\leq a\leq n-1$ حسب نتيجة (٢) مبرهنة (٣-٤-١) . والآن إذا كان n عدداً غير أولي ، فإن $n=ab$ ، $1<a<n$ ، $1<b<n$ حسب مبرهنة (٢-٢-١) ، وعليه فإن $(a,n)=a>1$ وهذا يناقض كون $(a,n)=1$. إذاً n عدد أولي .

□

نستنتج من مبرهنة فيرما ومبرهنة (٣-٥-٣) أن n عدد أولي إذاً وإذا فقط كان $a^{n-1} \equiv 1 (\text{mod } n)$ لكل $a \not\equiv 0 (\text{mod } n)$.

ونستنتج من مبرهنة (٣-٥-٣) أنه إذا كان $2^{n-1} \not\equiv 1 (\text{mod } n)$ ، فإن n ليس أولياً .

مثال (٧) :

(أ) 8 عدد غير أولي ، لأن $2^7 \not\equiv 1 \ (\text{mod } 8)$ ، $1 < 2 < 7$.

(ب) 323 ليس أولياً ، لأن $2^{322} \not\equiv 1 (\text{mod } 323)$.

(ج) إذا كان

$$n = 95468093486093450983409583409850434850938459083$$

فإن n ليس أولياً لأن $2^{n-1} \not\equiv 1 \ (\text{mod } n)$.

ولمزيد من التطبيقات نورد الآتي :

تعريف ٣-٥-١ :

يقال عن عدد صحيح مؤلف موجب n أنه شبه أولي (Pseudoprime) بالنسبة للأساس $a \in \mathbb{Z}^*$ ، إذا كان $a^{n-1} \equiv 1 \ (\text{mod } n)$.

مثال (٢) :

341 شبه أولي للأساس 2 .

الإثبات :

بما أن $341 = 11 \times 31$ و $(2,11) = (2,31) = 1$. إذاً

$$2^{10} \equiv 1 \ (\text{mod } 4) \ \Rightarrow \ 2^{340} \equiv 1 \ (\text{mod } 11)$$

$$2^{30} \equiv 1 \ (\text{mod } 31) \Rightarrow \ 2^{340} \equiv 1 \ (\text{mod } 31)$$

$$\Rightarrow \ 2^{340} \equiv 2^{10} \ (\text{mod } 31)$$

لكن $2^{10} \equiv 1 \ (\text{mod } 31)$. إذاً $2^{340} \equiv 1 \ (\text{mod } 31)$ ، وعليه فإن $2^{340} \equiv 1 \ \text{mod} (11 \times 31)$. أي أن $2^{340} \equiv 1 \ (\text{mod } 341)$ ، وعليه فإن 341 عدد شبه أولي .

طريقة أخرى : بما أن $2^{11} \equiv 1 \pmod{31}$ و $2^{10} \equiv 1 \pmod{11}$. إذاً $2^{30} \equiv 1 \pmod{11}$ ، وعليه فإن $2^{31} \equiv 2 \pmod{11}$ ، وبالتالي فإن $2^{11\times 31} \equiv 2 \bmod (11\times 31)$ حسب مبرهنة (٣-٥-٢) . إذاً $2^{341} \equiv 2 \pmod{341}$ لكن $(2,341) = 1$. إذاً $2^{340} \equiv 1 \pmod{341}$ ،وعليه فإن 341 عدد شبه أولي .

مثال (٣) :

645 شبه أولي للأساس 2 .

الإثبات : بما أن

$645 = 3 \times 5 \times 43$ ، $(2,3) = (3,5) = (2,43) = 1$. إذاً

$$2^{42} \equiv 1 \pmod{43} \Rightarrow 2^{630} = (2^{42})^{15} \equiv 1 \pmod{43}$$

$$2^2 \equiv 1 \pmod{3} \Rightarrow 2^{14} \equiv 1 \pmod{3}$$

وعليه فإن $2^{644} = 2^{630} \cdot 2^{14} \equiv 1 \bmod (3 \times 43)$. لكن $2^4 \equiv 1 \pmod{5}$. إذاً $2^{644} = (2^4)^{161} \equiv 1 \pmod{5}$ ، وعليه فإن $2^{644} \equiv 1 \bmod (3 \times 43 \times 5)$ أي أن $2^{644} \equiv 1 \pmod{645}$ ، وعليه فإن 645 عدد شبه أولي .

والآن إلى المبرهنة الآتية :

مبرهنة ٣-٥-٤ :

يوجد عدد لا نهائي من الأعداد شبه الأولية لأي أساس أكبر من الواحد .

البرهان :

ليكن $a > 1$ و p أي عدد أولي فردي لا يقسم $a(a^2-1)$ ، وليكن $n = \frac{a^{2p}-1}{a^2-1} = \frac{(a^p-1)}{a-1} \cdot \frac{(a^p+1)}{a+1}$. إذاً n عدد مؤلف .

كما أن $(a^2-1)(n-1) = a^{2p} - a^2 = a(a^{p-1}-1)(a^p+a)$. لكن a, a^p فرديان معاً أو زوجيان معاً ، $2 \backslash a^p + a$. لكن $p-1$ عدد زوجي . إذاً $(a^{p-1}-1)$ يقبل القسمة على P وعلى (a^2-1) . لكن (a^2-1) لا يقبل

القسمة على p بالفرض . إذاً $(a^{p-1}-1)$ يقبل القسمة على $p(a^2-1)$ ، وبالتالي فإن $(a^2-1)(n-1)$ يقبل القسمة على $2p(a^2-1)$ ، وعليه فإن $2p \setminus (n-1)$. إذاً يوجد $r \in Z$ بحيث أن $n = 1+2pr$ ، وعليه فإن $a^{2p} = 1+n(a^2-1) \equiv 1 (\mod n)$ ، ومنها نجد أن $a^{n-1} = a^{2pr} \equiv 1 (\mod n)$ وعليه فإن n عدد شبه أولي للأساس a .

□

وأخيراً إلى دراسة أعداد كارمايكل .

تعريف ٣-٥-٢ :

يقال عن مؤلف صحيح موجب n أنه عدد كارمايكل ، إذا كان $a^{n-1} \equiv 1 \ (\mod n)$ لكل $a \in Z$ ، $(a,n)=1$.

مثال (٤) :

561 عدد كارمايكل .

الحل :

بما أن $561 = 3 \times 11 \times 17$. إذاً إذا كان $a \in Z$ و $(a,3)=(a,11)=(a,17)=1$ فإن $a^2 \equiv 1 \ (\mod 3)$ ، $a^{10} \equiv 1 \ (\mod 11)$ ، $a^{16} \equiv 1 \ (\mod 17)$ حسب مبرهنة فيرما ، وعليه فإن $a^{560} = (a^2)^{280} \equiv 1 \ (\mod 3)$ ، $a^{560} = (a^{10})^{56} \equiv 1 \ (\mod 11)$ ، $a^{560} = (a^{16})^{35} \equiv 1 \ (\mod 17)$ ، وبالتالي فإن $a^{560} \equiv 1 \mod (3 \times 11 \times 17)$ وهذا يعني أن $a^{560} \equiv 1 \mod (561)$ ، وعليه فإن 561 عدد كارمايكل .

□

مثال (٥) :

1729 عدد كارمايكل .

الحل :

بما أن $1729 = 7 \times 13 \times 19$. إذاً إذا كان $a \in Z$ ، $(a,7)=(a,13)=(a,19)=1$ فإن

$$a^{6} \equiv 1 \pmod{7} \Rightarrow a^{1728} = (a^{6})^{288} \equiv 1 \pmod{7}$$
$$a^{12} \equiv 1 \pmod{13} \Rightarrow a^{1728} = (a^{12})^{144} \equiv 1 \pmod{13}$$
$$a^{18} \equiv 1 \pmod{19} \Rightarrow a^{1728} = (a^{18})^{96} \equiv 1 \pmod{19}$$

وعليه فإن $a^{1728} \equiv 1 \bmod (7 \times 13 \times 19)$ وهذا يعني أن $a^{1728} \equiv 1 \pmod{1728}$
وعليه فإن 1729 عدد كارمايكل .

ملاحظة :

يوجد عدد لا نهائي من أعداد كارمايكل أصغرها 561 ولإثبات ذلك أنظر $\text{Ann.Math.}139, 703-722\ (1994)$.

تمارين

(١) أوجد مرتبة آحاد العدد 3^{100} .

(٢) أثبت أن $2^{2n} \equiv 1 \pmod{3}$ ، $2^{3n} \equiv 1 \pmod{15}$ ، $2^{4n} \equiv 1 \pmod{15}$ لكل $n \geq 1$.

(٣) إذا كان $a, b \in \mathbb{Z}$ ، $p \nmid a$ ، $p \nmid b$ ، فأثبت أن :

(أ) $a^{p} \equiv b^{p} \pmod{p} \Rightarrow a \equiv b \pmod{p}$.

(ب) $a^{p} \equiv b^{p} \pmod{p} \Rightarrow a^{p} \equiv b^{p} \pmod{p^{2}}$.

" ملاحظة : أستخدم (أ) تجد أن $a = b + p^{r}$ ، $r \in \mathbb{Z}$ ، وعليه فإن $a^{p} - b^{p} = (b+p^{r})^{p} - b^{p}$ ، ثم اثبت أن $(b+p^{r}) - b^{p}$ يقبل القسمة على p^{2} .

(٤) حل كلاً مما يأتي :

(أ) $2x \equiv 1 \pmod{31}$ ، (ب) $3x \equiv 17 \pmod{29}$

(٥) إذا كان p عدداً أولياً فردياً ، فأثبت أن :

(أ) $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$

(ب) $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod p$

" لاحظ أن $1+2+\cdots+p-1 = \dfrac{p(p-1)}{2}$ "

(٦) إذا كان $(m,n)=1$ ، فأثبت أن $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

(٧) إذا كان p,q عددين أولين مختلفين وكان $(p-1) \backslash (q-1)$ ، $(a,pq)=1$ ، فأثبت أن $a^{q-1} \equiv 1 \pmod{pq}$.

(٨) إذا كان $(a,35)=1$ ، فأثبت أن $a^{12} \equiv 1 \pmod{35}$.

(٩) إذا كان $(a,42)=1$ ، فأثبت أن $168 \backslash (a^6 - 1)$.

(١٠) إذا كان $(a,133)=(b,133)=1$ ، فاثبت أن $133 \backslash (a^{18} - b^{18})$.

(١١) أوجد باقي قسمة $(28)^{1202}$ على 13 .

(١٢) أثبت أن $a^{2m-1} \equiv a^{2n-1} \pmod 3$ لكل $a \in Z$ ، $m,n \in Z^+$.

(١٣) أثبت أن كلاً من 1105 ، 1905 ، 4080 عدد شبه أولي للأساس 2 .

(١٤) أثبت أن كلاً من 2730 ، 6601 عدد كارمايكل .

(١٥) إذا كان p عدداً أولياً ، فأثبت أن $(a+b)^p \equiv a^p + b^p \pmod p$.

٣-٦ : مبرهنة ابن الهيثم " ولسن "

جون ولسن (١٧٤١-١٧٩٣م) رياضي إنجليزي تنسب له المبرهنة الآتية : إذا كان p عدداً أولياً ، فإن $(p-1)!+1 \equiv 0 \pmod p$ والتي نشرت بدون برهان من قبل الرياضي الإنجليزي إدوارد وارنغ (١٧٣٤-١٧٨٩م) عام ١٧٧٠م ويجمع الكل على أن كلاً من ولسن وورارنغ لا يمتلك برهاناً ، لكن الفرنسي لاجرانج (١٧٣٦-١٨١٣م) أثبت تلك المبرهنة عام ١٧٧١م بطريقتين إحداهما مباشرة والأخرى تقوم على استنتاج مبرهنة ولسن من مبرهنة فيرما .

وبدراسة أعمال الرياضي والفيزيائي والفيلسوف الألماني ليبتر (١٦٤٦-١٧١٦م) وجدت صيغة مكافئة وبدون إثبات لمبرهنة ولسن وهي : إذا كان p عدداً أولياً ، فإن $(p-2)!+1 \equiv (\text{mod } p)$.

وبدارسة أعمال الرياضي والفيزيائي الشهير الحسن بن الهيثم (٩٦٥-١٠٤٠م) تبين [٦ ، ٢٦٨-٢٧٥] أو [٣، ٧٠-٧١] أنه قد قدم أثناء حله للنظام الآتي : $x \equiv 1 \ (\text{mod } m_i)$ ، $x \equiv 0 \ (\text{mod } p)$ حيث p عدد أولي و $1 < m_i \leq (p-1)$ ، ما يعرف الآن بمبرهنة ولسن كقضية تعبر بدقة عن خاصية تمتاز بها الأعداد الأولية ، وبالصيغة الآتية : إذا كان p عدداً أولياً ، فإن $[2 \times 3 \times \cdots \times (p-1)+1]$ يقبل القسمة على p ، وإذا قسمنا هذا المجموع على أي من الأعداد $2,3,\cdots,(p-1)$ لكان الباقي واحد .

من الواضح أن هذه المبرهنة تعطي حلاً للنظام أعلاه ، وهذا يعني أن $x \equiv (p-1)!+1$ تحقق معادلتي النظام أعلاه .

لاحظ أن ابن الهيثم برهن على وجود حل أو عدة حلول للنظام أعلاه بطريقتين ، وما يهمنا هنا هو إثباته لما يسمى مبرهنة ولسن . وسنقدم برهان ابن الهيثم بعد أعادة صياغته ، ثم نعطي برهان لاجرانج لتلك المبرهنة ثم نثبت عكس تلك المبرهنة .

<u>مبرهنة ٣-٦-١</u> : " مبرهنة ابن الهيثم "

إذا كان p عدداً أولياً ، فإن $(p-1)!+1 \equiv 0 \ (\text{mod } p)$.

<u>البرهان</u> : " ابن الهيثم "

لتكن $a \in A = \{1,2,\cdots,(p-1)\}$ سنبرهن على وجود عنصر وحيد $b \in A$ بحيث أن $ab \equiv 1 (\text{mod } p)$ ، لإثبات ذلك لاحظ أن $(a,p)=1$ يعني وجود عددين صحيحين x,y بحيث أن $ax+py=1$. إذاً $ax \equiv 1 \ (\text{mod } p)$

وإذا كان b باقي القسمة x على p فإن b وحيد ، وأن $b \in A$ ويحقق العلاقة $ab \equiv 1 \pmod p$ لكن a,b قد يكونان متساويين وفي هذه الحالة نجد أن $a^2 \equiv 1 \pmod p$ ، $a \in A$ يعني أن $a \equiv 1 \pmod p$ أو $a \equiv -1 \pmod p$ إذاً $a = 1$ أو $a = p - 1$ ، وعليه فإن لكل $a \in A$ بحيث أن $a \neq 1$ ، $a \neq p - 1$ يوجد $b \in A$ ، $b \neq a$ بحيث أن $ab \equiv 1 \pmod p$ ، وهذا يعني أنه بعد ضرب كل عنصر من عناصر المجموعة $\{2,3,\cdots,p-2\}$ في معكوسة ، نجد أن $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod p$ ، وعليه فإن $2 \cdot 3 \cdots (p-2)\,(p-1) \equiv p-1 \pmod p$ ، ومنها نجد أن $(p-1)! \equiv p-1 \pmod p$. لكن $p \equiv 0 \pmod p$. إذاً $p - 1 \equiv -1 \pmod p$ ، وعليه فإن $(p-1)! \equiv -1 \pmod p$ ، وهذا يعني أن $(p-1)! + 1 \equiv 0 \pmod p$.

□

برهان لاجرانج :

بما أن $x^p \equiv x \pmod p$ حسب مبرهنة فيرما . إذاً $x^{p-1} \equiv 1 \pmod p$ لكل $x \in A = \{1,2,\cdots,p-1\}$ ، وعليه فإن $x^{p-1} - 1 \equiv 0 \pmod p$ لكل $x \in A$ ، وبالتالي فإن $x^{p-1} - 1 \equiv (x-1)\,(x-2)\cdots[x-(p-1)] \equiv 0 \pmod p$ وبمقارنة المعاملات نجد أن معامل الحد الخالي من x في الطرفين هو $-1 \equiv (-1)\,(-2)\,(-3)\cdots(-1)\,(p-1) \pmod p$ ، وعليه فإن $(-1)^{p-1}\,(p-1)! \equiv -1 \pmod p$.

فإذا كان $p = 2$ ، فإن $1 \equiv -1 \pmod 2$. أما إذا كان p عدداً فردياً ، فإن $(p-1)$ عدد زوجي ، وعليه فإن $(-1)^{p-1} = 1$ ، وبالتالي فإن $(p-1)! \equiv -1 \pmod p$. إذاً $(p-1)! + 1 \equiv 0 \pmod p$ لأي عدد أولي p .

□

<u>مبرهنة ٣-٦-٢</u> : " عكس مبرهنة ابن الهيثم "

إذا كان n عدداً موجباً ، وكان $(n-1)!+1 \equiv 0 \pmod{n}$ ، فإن n عدد أولي .

<u>البرهان :</u>

نفرض أن $(n-1)!+1 \equiv 0 \pmod{n}$. لكن n ليست أولياً . إذاً يوجد عدد أولي p بحيث أن $p \backslash n$ حسب مبرهنة (٢-٢-٤أ) ، وعليه فإن $p < n$ وبالتالي فــإن $p \backslash (n-1)!$ ، وهــذا يعنــي أن $(n-1)! \equiv 0 \pmod{p}$. لكــن $(n-1)!+1 \equiv 0 \pmod{n}$ و $p \backslash n$. إذاً $(n-1)! \equiv 0 \pmod{p}$ ، عليــه فإن $1 \equiv 0 \pmod{p}$ وهذا غير ممكن . إذاً n عدد أولي .

□

<u>مثال (١) :</u>

أوجد باقي قسمة $96!$ على 97 .

<u>الحل :</u>

بما أن 97 عدد أولي . إذاً $(97-1)! \equiv -1 \pmod{97}$ حــسب مبرهنــة ابــن الهيثم ، وعليه فإن $96! \equiv -1 \pmod{97}$. لكــن $-1 \equiv 96 \pmod{97}$. إذاً $96! \equiv 96 \pmod{97}$ ، وعليه فإن باقي قسمة $96!$ على 97 يساوي 96 .

<u>مثال (٢) :</u>

إذا كان p عدداً أولياً ، $a \in Z$ ، فأثبت أن $a^p + (p-1)!\, a \equiv 0 \pmod{p}$.

<u>الإثبات :</u>

بمــا أن $(p-1)! \equiv -1 \pmod{p}$ حــسب مبرهنــة ابــن الهيــثم . إذاً $(p-1)!\, a \equiv -a \pmod{p}$ حــسب مبرهنــة (٣-١-٣د) ، وعليــه فــإن $a^p + (p-1)!\, a \equiv a^p - a \pmod{p}$ حسب مبرهنة (٣-١-٣ج) .

والآن إلى بعض تطبيقات مبرهنة ابن الهيثم والمبرهنة الآتية :

مبرهنة ٣-٦-٣ :

إذا كان p عدداً أولياً فردياً ، فيوجد للتطابق $x^2+1\equiv 0 \pmod p$ حل إذاً إذا فقط كان $p\equiv 1 \pmod 4$.

البرهان :

نفرض أن a حل للتطابق $x^2+1\equiv 0 \pmod p$. إذاً $a^2\equiv -1 \pmod p$ ، وعليه فإن $a^{p-1}=(a^2)^{\frac{p-1}{2}}=(-1)^{\frac{p-1}{2}} \pmod p$. لكن $p\setminus a$. إذاً $a^{p-1}\equiv 1 \pmod p$ حسب مبرهنة فيرما ، وعليه فإن $(-1)^{\frac{p-1}{2}}\equiv 1 \pmod p$ لكن p عدد أولي فردي . إذاً $(p-1)$ عدد زوجي ، وعليه فإن $(-1)^{\frac{p-1}{2}}=1$ أو $(-1)^{\frac{p-1}{2}}=-1$. فإذا كان $(-1)^{\frac{p-1}{2}}=-1$ ، فإن $-1\equiv 1 \pmod p$ يعني أن $p\setminus 2$ ، ومنها نجد أن $p=2$ وهذا خلاف الفرض . إذاً $(-1)^{\frac{p-1}{2}}\neq -1$ ، وعليه فإن $(-1)^{\frac{p-1}{2}}=1$ وهذا يعني أن $\frac{p-1}{2}$ عدد زوجي . إذاً يوجد $m\in Z$ بحيث أن $\frac{p-2}{2}=2m$ ، وعليه فإن $p-1=4m$ ، وهذا يعني أن $p\equiv 1 \pmod 4$.

ولإثبات العكس ، لاحظ أن

$(p-1)!=1\cdot 2\cdots\frac{p-1}{2}\cdot\frac{p+1}{2}\cdots(p-2)(p-1)$ ، $p-1\equiv -1 \pmod p$ ، $p-2\equiv -2 \pmod p$ ، ... ، $\frac{p+1}{2}\equiv -\frac{p-1}{2} \pmod p$. إذاً

$(p-1)!\equiv 1\cdot(-1)\cdot 2\cdot(-2)\cdots\frac{p-1}{2}\cdot(-\frac{p-1}{2}) \pmod p$ ، وعليه فإن

$(p-1)!\equiv(-1)^{\frac{p-1}{2}}[(\frac{p-1}{2})!]^2 \pmod p$. لكن $p\equiv 1 \pmod 4$. إذاً

يوجد $m \in \mathbb{Z}$ بحيث أن $p-1=4m$ ، وعليه فإن $\frac{p-1}{2}=2m$ ، وبالتالي فإن $(-1)^{\frac{p-1}{2}}=1$. إذاً $(p-1)!\equiv[(\frac{p-1}{2})!]^2 \pmod p$. لكن $(p-1)!\equiv -1 \pmod p$ حسب مبرهنة ابن الهيثم . إذاً $[(\frac{p-1}{2})!]^2+1\equiv 0 \pmod p$. فإذا كان $x=(\frac{p-1}{2})!$ ، فإن $x^2+1\equiv 0 \pmod p$ ، وعليه فإن $x=(\frac{p-1}{2})!$ حل للتطابق $x^2+1\equiv 0 \pmod p$.

□

نتيجة :

يوجد عدد لا نهائي من الأعداد الأولية التي على الشكل $4n+1$.

البرهان :

نفرض وجود عدد منتهي الأعداد الأولية التي على الشكل $4n+1$ وهي $p_1,p_2,\cdots,p_r$ ولنفرض أن $a=(2\prod_{i=1}^{r}p_i)^2+1$. إذاً $a>1$ ، عليه يوجد عدد أولي $p>2$ بحيث أن $p \setminus a$ حسب مبرهنة (٢-٢-٤أ) ، وعليه فإن $a\equiv 0 \pmod p$ ، ومنها ينتج أن $(2\prod_{i=1}^{r}p_i)^2+1\equiv 0 \pmod p$ ، وعليه فإن p على الشكل $4n+1$ حسب مبرهنة (٣-٦-٣) . لكن $p_1,\cdots,p_r$ هي جميع الأعداد الأولية على الشكل $(4n+1)$. إذاً يوجد $1\le j\le r$ بحيث أن $p=p_j$ ، وعليه فإن $p_j \setminus a$. لكن $p_j \setminus (2\prod_{i=1}^{r}p_i)^2$. إذاً $p_j \setminus 1$ وهذا غير ممكن . إذاً يوجد عدد لا نهائي من الأعداد الأولية التي على الشكل $(4n+1)$.

□

مثال (٣) :

حل التطابق $x^2+1\equiv 0 \pmod{13}$.

الحل :

بمـــا أن $13\equiv 1 \pmod 4$. إذاً يوجـــد حـــل للتطـــابق أعـــلاه وهـــو $x=(\frac{p-1}{2})!=6!=5 \pmod{13}$. لاحظ أن $x=-5=8 \pmod{13}$ حـل آخر لذلك التطابق .

ملاحظة : لحل التطابق

$ax^2+bx+c\equiv 0 \pmod n$ ... (1) ، $(a,p)=1$ ، p عدد أولي فردي .

لاحظ أن $(4a,p)=1$. إذاً

$$ax^2+bx+c\equiv 0 \pmod n \Rightarrow 4a(ax^2+bx+c)\equiv 0 \pmod p$$
$$\Rightarrow 4a^2x^2+4abx+4ac\equiv 0 \pmod p$$
$$\Rightarrow 4a^2x^2+4abx+b^2\equiv b^2-4ac \pmod p$$
$$\Rightarrow (2ax+b)^2\equiv b^2-4ac \pmod p$$

فإذا فرضنا أن $y=2ax+b$ ، $d=b^2-4ac$ ، فإن

$$y^2\equiv d \pmod p \qquad \dots (2)$$

وإذا كان $x\equiv x_1 \pmod p$ حلاً للعلاقة (1) ، فـإن $y=2ax_1+b \pmod p$ تحقق العلاقة (2) ، وبالعكس إذا كان $y\equiv y_1 \pmod p$ حلاً للعلاقة (2) ، فإن حل التطابق $2ax\equiv y_1-b \pmod p$ يعطي حلاً للتطابق (1) .

إذاً وجود حل للتطابق (1) يكافئ وجود حل لتطابق خطي وحل للتطـابق علـى الشكل $x^2\equiv a \pmod p$.

مثال (٤) :

حل التطابق $3x^2-4x+2\equiv 0 \pmod{11}$.

الحل :

$$3x^2-4x+2\equiv 0 \pmod{11} \Rightarrow 3(3x^2-4x+2)\equiv 0 \pmod{11}$$
$$\Rightarrow 9x^2-12x+6\equiv 0 \pmod{11}$$
$$\Rightarrow (3x-2)^2+2\equiv 0 \pmod{11}$$
$$\Rightarrow (3x-2)^2\equiv -2\equiv 9 \pmod{11}$$
$$\Rightarrow 3x-2\equiv 3 \pmod{11} \vee 3x-2\equiv -3 \pmod{11}$$
$$\Rightarrow 3x\equiv 5 \pmod{11} \vee 3x\equiv 10 \pmod{11}$$
$$\Rightarrow x\equiv 5\cdot 3^{-1} \pmod{11} \vee x\equiv 10\cdot 3^{-1} \pmod{11}$$

لكن $3^{-1}=3^9=4 \pmod{11}$ حسب نتيجة (٣) من مبرهنة (٣-٥-١) . إذاً

$$x\equiv 5\cdot 3^{-1}=20\equiv 9 \pmod{11} \vee x\equiv 10\cdot 4=40\equiv 4 \pmod{11}$$

مثال (٥) :

حل التطابق $x^2+3x-2\equiv 0 \pmod{13}$.

الحل :

$$x^2+3x-2\equiv 0 \pmod{13} \Rightarrow 4(x^2+3x-2)\equiv 0 \pmod{13}$$
$$\Rightarrow 4x^2+12x-8\equiv 0 \pmod{13} \Rightarrow (2x+3)^2\equiv 4 \pmod{13}$$
$$\Rightarrow 2x+3\equiv 2 \pmod{13} \vee 2x+3\equiv -2 \pmod{13}$$
$$\Rightarrow 2x\equiv -1 \pmod{13} \quad \vee 2x\equiv -5\equiv 8 \pmod{13}$$
$$\Rightarrow x\equiv 6 \pmod{13} \quad \vee x\equiv 4 \pmod{13}$$ (لأن $(2,13)=1$)

تمـــــــارين

(١) إذا كان p عدداً أولياً ، فأثبت أن $(p-2)!\equiv 1 \pmod p$.

(٢) أوجد باقي قسمة كلاً من !100 ، !99 على 101 .

(٣) أثبت أن $(29!)^2\equiv 1 \pmod{59}$ ، بينما $(30!)^2\equiv -1 \pmod{61}$.

(٤) إذا كان p عدداً أولياً ، فأثبت أن $(p-1)!\equiv p-1 \bmod \frac{p(p-1)}{2}$.

(٥) أوجد باقي قسمة $2(34)!$ على 37 .
" لاحظ أن $2\,(p-3)!\equiv -1 \pmod{p}$ لكل عدد أولي p أكبر من 3 " .

(٦) أوجد عددين أوليين فرديين أقل من أو يساوي 17 بحيث $(p-1)!\equiv -1 \pmod{p^2}$.

(٧) إذا كان p عدداً أولياً فردياً و m عدداً صحيحاً موجباً ، $m \le P$ ، فأثبت أن $(p-m)!(m-1)!\equiv (-1)^m \pmod{p}$.

(٨) إذا كان p عدداً أولياً فردياً ، فأثبت أن :

(أ) $1^2\cdot 3^2\cdot 5^2\cdots(p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

(ب) $3^2\cdot 4^2\cdot 6^2\cdots(p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

" لاحظ أن $m = -(p-1) \pmod{p}$
$\Rightarrow 2\cdot 4\cdot 6\cdots(p-1)\equiv (-1)^{p-1}\cdot 3\cdot 5\cdots(p-2) \pmod{p}$ "

(٩) إذا كان $p\equiv 3 \pmod{4}$ عدداً أولياً و $a^2+b^2\equiv 0 \pmod{p}$ ، فأثبت أن $a\equiv b\equiv 0 \pmod{p}$. " لاحظ أنه إذا كان $a\not\equiv 0 \pmod{p}$ ، فإن $(a,p)=1$ ، وعليه ويوجد $c\in Z$ بحيث أن $ac\equiv 1 \pmod{p}$. ثم أستخدم تلك العلاقة لمناقضة مبرهنة (٣-٦-٣) " .

(١٠) حل كلاً مما يأتي

(أ) $x^2+1\equiv 0 \pmod{29}$ ، (ب) $x^2+1\equiv 0 \pmod{37}$

(ج) $x^2+7x+10\equiv 0 \pmod{11}$ ، (د) $4x^2+x+4\equiv 0 \pmod{5}$

(هـ) $7x^2-x+11 \pmod{7}$ ، (و) $5x^2-6x+2\equiv 0 \pmod{17}$

(ز) $3x^2+5x-9\equiv 0 \pmod{13}$ ، (ح) $5x^2+6+1\equiv 0 \pmod{23}$

****

الفصل الرابع

الدوال العددية Arithmetic Functions

تكمن أهمية الدوال العديدة في تطبيقاتها في العلوم الرياضية والفيزيائية والفلك ، ويضم هذا الفصل خمسة بنود ، ندرس فيها مفهوم الدالة العددية وخواصها ثم الدوال العددية الأساسية : مجموع وعدد قواسم عدد طبيعي ، دالة أويلر ، دالة موبيص ، دالة زيتا .

٤-١ : تعاريف وخواص

سنركز أهتمامنا في هذا الجزء على دراسة مفهوم الدالة العددية ، الدوال الضربية وخواصها .

تعريف ٤-١-١ :

يقال عن دالة $f : Z^+ \to B$ أنها دالة عددية (Arithmetic or number theoretic or numerical function) ، إذا كانت $B \le C$ ، حيث $C = \{a + ib \mid a, b \in R\}$ مجموعة الأعداد المركبة (Complex numbers) .

مثال (١) :

(أ) $\phi(n) = \left| \{ m \in Z^+ : 1 \le m \le n \, , \, (m,n) = 1 \} \right|$ دالة عددية .

(ب) كل من $f , g : Z^+ \to N$ ، حيث $f(a) = a^n$ ، $g(a) = log(a)$ لكل $a \in Z^+$ دالة عددية .

تعريف ٤-١-٢ :

يقال عن دالة عددية غير صفرية أنا دالة ضربية (multiplicative function) إذا كان $f(ab) = f(a) \cdot f(b)$ لكل $a, b \in Z^+$ و $(a, b) = 1$.

أما إذا كان $f(ab) = f(a) \cdot f(b)$ لكل $a, b \in Z^+$ فتسمى f دالة ضربية كلياً أو تاماً (Totally or completely multiplicative function).

مثال (١) :

(أ) $f : Z^+ \to Z^+$ حيث $f(a) = a^n$ لكل $a \in Z^+$ دالة ضربية كلياً ، لأن $f(ab) = (ab)^n = a^n \cdot b^n = f(a) \cdot f(b)$ لكل $a, b \in Z^+$.

(ب) $f : Z^+ \to R$ حيث $f(a) = log(a)$ دالة عددية ليست ضربية ، لأن $f(ab) = log(ab) \neq log(a) \cdot log(b) = f(a) \cdot f(b)$.

والآن إلى بعض خواص الدوال العددية .

مبرهنة ٤-١-١ :

إذا كانت f دالة ضربية ، فإن $f(1) = 1$.

البرهان :

بما أن f دالة ضربية بالفرض ، إذاً يوجد $a \in Z^+$ ، بحيث أن $f(a) \neq 0$ وعليه فإن $f(a) = f(a \cdot 1) = f(a) \cdot f(1)$ ، ومنها نجد أن $f(1) = 1$.

□

ملاحظة :

عكس مبرهنة (٤-١-١) ليس صحيحاً كما يوضح ذلك المثال الآتي :
لتكن $p : Z^+ \to Z^+$ حيث $p(n)$ يساوي عدد طرق تجزئة العدد n " يقال عن متتابعة $1 \le n_1 \le n_2 \le \cdots \le n_r$ أنها تجزئة للعدد n ، إذا كان $n = \sum_{i=1}^{r} n_i$ " . لاحظ أن

$p(1) = 1$ لكن p ليست دالة ضربية ، لأن $(2,3) = 1$

$$11 = p(6) = p(2 \times 3) \neq p(2) \times p(3) = 2 \times 3 = 6$$

تعريف ٤-١-٣ :

$\sum_{d\backslash a} f(d) =$ (مجموعة قيم الدالة f لكل قواسم العدد a)

فمثلاً إذا كان $a = 8$ ، فإن $\sum_{d\backslash 8} f(d) = f(1) + f(2) + f(4) + f(8)$

مبرهنة ٤-١-٢ :

إذا كانت f, g دالتين عدديتين ، فإن $\sum_{c\backslash a، d\backslash b} f(c)g(d) = \sum_{c\backslash a} f(c) \cdot \sum_{d\backslash b} g(d)$

البرهان :

لتكن $d_1, d_2, \cdots d_r$ جميع قواسم العدد b . إذاً

$$\sum_{c\backslash a، d\backslash b} f(c)g(d) = \sum_{c\backslash a} f(c) \cdot g(d_1) + \sum_{c\backslash a} f(c)g(d_2) + \cdots + \sum_{c\backslash a} f(c)g(d_r)$$

$$= \sum_{c\backslash a} f(c)\left[g(d_1) + g(d_2) + \cdots + g(d_r)\right]$$

$$= \sum_{c\backslash a} f(c) \cdot \sum_{d\backslash b} g(d)$$

□

والآن لتكن f دالة ضربية ، $a = 12$. إذاً $a = 4 \times 3$ ، $(4,3) = 1$ ، وعليه فإن

$$g(12) = \sum_{d\backslash 12} f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$$

$$= f(1 \cdot 1) + f(2 \cdot 1) + f(3 \cdot 1) + f(4 \cdot 1) + f(2 \cdot 3) + f(4 \cdot 3)$$

$$= f(1) \cdot f(1) + f(2) \cdot f(1) + f(3) \cdot f(1) + f(4) \cdot f(1) + f(2) \cdot f(3) + f(4) \cdot f(3)$$

$$= \left[f(1) \cdot f(1) + f(3) \cdot f(1)\right] + \left[f(1) \cdot f(2) + f(2) \cdot f(3)\right] + \left[f(4) \cdot f(1) + f(4) \cdot f(3)\right]$$

$$= f(1)\left[f(1) + f(3)\right] + f(2)\left[f(1) + f(3)\right] + f(4)\left[f(1) + f(3)\right]$$

$$= \left[f(1) + f(3) + f(4)\right]\left[f(1) + f(3)\right]$$

$$= \sum_{d\backslash 4} f(d) \cdot \sum_{d\backslash 3} f(d) = g(4) \cdot g(3)$$

وعليه فإن g دالة ضربية وبصورة عامة يمكن أن نبرهن ما يلي :

مبرهنة ٤-١-٣ :

إذا كانت f دالة ضربية ، فإن $g(a) = \sum_{d\backslash a} f(d)$ دالة ضربية .

البرهان :

نفرض أن $a,b\in\mathbb{Z}^+$ ، $(a,b)=1$. إذاً $g(ab)=\sum_{d\backslash ab} f(d)$. لكن $(a,b)=1$ ، $d\backslash ab$. إذاً يوجد عددان موجبان وحيدان c,e بحيث أن $c\backslash a$، $e\backslash b$ ، $d=ce$ ، $(c,e)=1$ حسب مبرهنة (٢-٣-٢) ، وعليه فإن $g(ab)=\sum_{\substack{c\backslash a\\ e\backslash b}} f(ce)$. لكن f دالة ضربية . إذاً $f(ce)=f(c)\cdot f(e)$ ، وعليه فإن $g(ab)=\sum_{\substack{c\backslash a\\ e\backslash b}} f(c)\cdot f(e)$. لكن $\sum_{\substack{c\backslash a\\ e\backslash b}} f(c)\,f(e)=\sum_{c\backslash a} f(c)\cdot\sum_{e\backslash b} f(e)$ حسب مبرهنة (٤-١-٢) . إذاً $g(ab)=\sum_{a\backslash c} f(c)\cdot\sum_{e\backslash b} f(e)=g(a)\cdot g(b)$ ، وعليه فإن g دالة ضربية .

□

تمـــارين

(١) إذا كانت f,g دالتين ضربيتين ، $g(a)\neq 0$ لكل $a\in\mathbb{Z}$ ، فأثبت أن كلاً من $f\cdot g$ ، f/g دالة ضربية .

(٢) إذا كانت f دالة ضربية وكان $a_1,a_2,\cdots,a_r\in\mathbb{Z}^+$ ، $(a_i\,,a_j)=1$ لكل $i\neq j$ ، فأثبت بالاستقراء أن $f(\prod_{i=1}^{r} a_i)=\prod_{i=1}^{r} f(a_i)$. واستنتج من ذلك أنه إذا كان $a=\prod_{i=1}^{r} p^{\alpha_i}$ ، p_i أعداد أولية ، فإن $f(a)=\prod_{i=1}^{r} f(p_i^{\alpha_i})$.

(٣) إذا كانت

$$\wedge(n)=\begin{cases} \ln p & n=p^m \\ 0 & n\neq p^m \end{cases}$$

. تسمى هذه الدالة دالة مانجولد (Mangoldt) . فأثبت أن $\wedge$ دالة ليست ضربية و $\sum_{d\backslash n}\wedge(d)=\ln(n)$.

(٤) لتكن f دالة معرفة كالآتي

$$f(a)=\begin{cases} 0 & \text{عدد زوجي } a \\ 1 & \text{عدد فردي } a \end{cases} \quad . \text{ ولتكن } \quad g(a)=\sum_{d\backslash a} f(a) \ .$$

(أ) أثبت أن كلاً من f ، g دالة ضربية . (ب) أحسب $g(16)$ ، $g(2^m)$.

(ج) أحسب $g(81)$ ، $g(p^m)$ لكل عدد أولي فردي p .

(٥) إذا كان λ دالة معرفة كالآتي

$$\lambda(n)=\begin{cases} 1 & n=1 \quad \text{إذا كان} \\ (-1)^{e_1+e_2+\cdots+e_r} & n=\prod_{i=1}^{r} p_i^{e_i}>1 \quad \text{إذا كان} \end{cases}$$

تسمى λ دالة ليوفيلي نسبة للفرنسي جوزيف ليوفيلي (١٨٠٩-١٨٨٢م) .

(أ) أحسب $\lambda(4500)$, $\lambda(180)$, $\lambda(39)$.

(ب) أثبت أن λدالة ضريبية .

(ج) أثبت أن

$$\sum_{d\backslash n}\lambda(d)=\begin{cases} 1 & n=m^2 \ , \ m\in Z \\ 0 & n\neq m^2 \end{cases}$$

٤-٢ : الدالتان مجموع وعدد قواسم عدد طبيعي

Sum and number of divisors

لقد جمع العالم الفيزيائي والرياضي كمال الدين الفارسي (ت ١٣٢٠م) في بحثه "تذكره الأحباب في تمام التحاب ، [٣] أو [٥،٤٩١-٥٣٨] " القضايا الضرورية لتمييز الدالتين العدديتين مجموع قواسم عدد صحيح وعدد هذه القواسم ، ومع أن الفارسي لم يعالج سوى $\sigma^*(n)$ التي تمثل مجموع أجزاء أو القواسم الفعلية للعدد n ، نلاحظ معرفته للدالة العددية $\sigma(n)$ التي تمثل مجموع قواسم العدد n علـــى أنها دالة ضربية ، فقد أثبت :

(١) إذا كان $n = ab$ ، $(a,b)=1$ ، فإن
$\sigma^*(n) = a\sigma^*(b) + b\sigma^*(a) + \sigma^*(a)\cdot\sigma^*(b)$ مما يدل على معرفته بالعبارة $\sigma(ab) = \sigma(a)\cdot\sigma(b)$.

(٢) إذا كان $n = ap$ ، p عدداً أولياً ، $(a,p)=1$ ، فإن
$\sigma^*(n) = p\sigma^*(a) + \sigma^*(a) + a$.

(٣) إذا كان $n = p^r$ ، p عدداً أولياً ، فإن $\sigma^*(n) = \sum_{k=0}^{r-1} p^k = \dfrac{p^r - 1}{p-1}$
وهذه القضايا منسوبة إلى الفرنسي ديكارت (١٥٩٦-١٦٥٠م) .

(٤) إذا كان $n = p_1 p_2 \cdots p_r$ حيث $p_1, \cdots, p_r$ أعداد أولية مختلفة فإن عدد أجزاء n المسمى $\tau_0(n)$ يساوي $1 + \binom{r}{1} + \cdots + \binom{r}{r-1}$
وهذه قضية منسوبة إلى الفرنسي دايديّ Deidierr .

(٥) إذا كان $n = \prod_{i=1}^{r} p_i^{e_i}$ ، فإن عدد قواسم n هو $\tau(n) = \prod_{i=1}^{r}(e_i + 1)$ ، $\tau_0(n) = \tau(n) - 1$ وهذه قضية منسوبة إلى جون كيرسي (John keresy) ومونتمورت (Montmort) .

والآن إلى دراسة خواص الدالتين σ ، τ .

<u>تعريف ٤-٢-١ :</u>

إذا كان n عدد صحيحاً موجباً ، فيرمز لعدد قواسم n بالرمز $\tau(n)$ ولمجموع قواسم n بالرمز $\sigma(n)$.

إذاً $$\tau(n) = \sum_{d\backslash n} 1 \ , \ \sigma(n) = \sum_{d\backslash n} d$$

<u>مثال (١) :</u>

(أ) $\sigma(1) = 1 \quad , \quad \sigma(2) = 1+2 = 3 \quad , \quad \sigma(3) = 1+3 = 4$
$\sigma(4) = 1+2+4 = 7 \quad , \quad \sigma(6) = 1+2+3+6 = 12$.

(ب) $\tau(1)=1\ ,\ \tau(2)=2\ ,\ \tau(4)=3\ ,\ \tau(6)=4$.

(ج) إذا كان $n=2^3$ ، فإن $\tau(n)=4$ ،

$\sigma(n)=1+2+2^2+2^3=2^4-1=17$.

ملاحظة :

(١) $\sigma(n)=n+1 \Leftrightarrow n$ عدد أولي .

(٢) $\tau(n)=2 \Leftrightarrow n$ عدد أولي .

مبرهنة ٤-٢-١ :

كل من τ ، σ دالة ضربية .

البرهان :

(أ) لتكن $f(n)=1$ لكل $n\in Z^+$. إذاً f دالة ضربية لأن $f(mn)=1=1\cdot 1=f(m)\cdot f(n)$ ، وعليه فإن $\tau(n)=\sum_{d\backslash n} f(d)=\sum_{d\backslash n} 1$ دالة ضربية حسب مبرهنة (٤-١-٣) .

(ب) لتكن $g(n)=n$ لكل $n\in Z^+$. إذاً g دالة ضربية وعليه فإن $\sigma(n)=\sum_{d\backslash n} g(d)=\sum_{d\backslash n} d$ دالة ضربية حسب مبرهنة (٤-١-٣) .

□

ملاحظة :

يمكن أن نثبت أن σ دالة ضربية بدون استخدام مبرهنة (٤-٢-٣) كالآتي :
نفرض أن $a,b\in Z^+$ ، $(a,b)=1$. إذاً d/ab إذا وإذا فقط كان $d=ce$ ، $d=ce$ ، $c\backslash a$ ، $e\backslash b$ و $(c,e)=1$ حسب مبرهنة (٢-٣-٢) .
وعليه فإن قواسم ab هي ضرب قواسم a في قواسم b . فإذا كانت $1\ ,a_1\ ,\cdots,a_r$ هي جميع قواسم a و $1\ ,b_1\ ,\cdots,b_s$ هي جميع قواسم b ، فإن قواسم ab هي :

$$\left.\begin{array}{l} 1, a_1, \cdots, a_r \\ b_1, a_1 b_1, \cdots, a_r b_1 \\ b_2, a_1 b_2, \cdots, a_r b_2 \\ \vdots \quad \vdots \quad \vdots \\ b_2, a_1 b_s, \cdots, a_r b_s \end{array}\right\} \quad \ldots (1)$$

لكن $(a,b)=1$. إذاً $a_i b_j = a_k b_t \Rightarrow a_i = a_k , b_j = b_t$ ، وعليه لا يوجد تكرار في (1) . والآن

$$\sigma(ab) = (1+a_1+\cdots+a_r)+(b_1+a_1b_1+\cdots+a_rb_1)+\cdots$$
$$+(b_1+a_1b_s+\cdots+a_rb_s)$$
$$=(1+a_1+\cdots+a_r)+b_1(1+a_1+\cdots+a_r)+\cdots$$
$$+b_s(1+a_1+\cdots+a_r)$$
$$=(1+a_1+\cdots+a_r)\,(1+b_1+\cdots+b_s)=\sigma(a)\cdot\sigma(b)$$

□

مبرهنة ٤-٢-٢ :

إذا كان $n = p^r$ ، p عدداً أولياً فإن :

(أ) $\tau(n) = r+1$ ، (ب) $\sigma(n) = \dfrac{p^{r+1}-1}{p-1}$.

البرهان :

بما أن p عدد أولي . إذاً قواسم n هي $1, p, p^2 + \cdots + p^r$ ، وعليه فإن

$$\tau(n) = r+1 \;, \sigma(n) = 1+p+p^2+\cdots+p^r = \frac{p^{r+1}-1}{p-1}$$

□

مبرهنة ٤-٢-٣ : " الفارسي "

إذا كان $n = \prod_{i=1}^{r} p_i^{e_i}$ ، فإن :

(أ) $\tau(n) = \prod_{i=1}^{r}(e_i+1)$ ، (ب) $\sigma(n) = \prod_{i=1}^{r} \dfrac{p_i^{e_i+1}-1}{p_i-1}$.

البرهان : (بالأستقراء) على r .

إذا كان $r=1$ ، فإن العبارة صحيحة حسب مبرهنة (٤-٢-٢) .

والآن لنفرض أن العبارة صحيحة عندما $1 \le r \le m$ ، ولإثبات صحتها عندما $r=m+1$. لنفرض أن $n=\prod_{i=1}^{m+1} p_i^{e_i}$. إذاً $n=(\prod_{i=1}^{m+1} p_i^{e_i})\cdot p_i^{e_{m+1}}$. لكن $(\prod_{i=1}^{m+1} p_i^{e_i}, p_{m+1}^{e_{m+1}})=1$ وكلاً من τ,σ دالة ضربية . إذاً

$$\tau(n)=\tau(\prod_{i=1}^{m} p_i^{e_i})\cdot\tau(p_{m+1}^{e_{m+1}})$$

$$\sigma(n)=\sigma(\prod_{i=1}^{m} p_i^{e_i})\cdot\sigma(p_{m+1}^{e_{m+1}})$$

لكن $\tau(\prod_{i=1}^{m} p_i^{e_i})=\prod_{i=1}^{m}(e_i+1)$ ، $\sigma(\prod_{i=1}^{m} p_i^{e_i})=\prod_{i=1}^{m}\frac{p_i^{e_i+1}-1}{p_i-1}$ حسب فرضية الأستقراء ، و $\tau(p_{m+1}^{e_{m+1}})=e_{m+1}+1$ ، $\sigma(p_{m+1}^{e_{m+1}})=\frac{p_{m+1}^{e_{m+1}+1}-1}{p_{m+1}-1}$. إذاً

$$\tau(n)=\prod_{i=1}^{m}(e_i+1)(e_{m+1}+1)=\prod_{i=1}^{m+1}(e_i+1)$$

$$\sigma(n)=(\prod_{i=1}^{m}\frac{p_i^{e_i+1}-1}{p_i-1})\cdot\frac{p_{m+1}^{e_{m+1}+1}-1}{p_{m+1}-1}=\prod_{i=1}^{m+1}\frac{p_i^{e_i+1}}{p_i-1}$$

وعليه فإن العبارة صحيحة عندما $r=m+1$ ، وبالتالي فإن العبارة صحيحة لكل $r \ge 1$.

مثال (٢) :

أحسب $\tau(120)$ ، $\sigma(120)$.

الحل :

بما أن $120=2^3\times3^1\times5^1$ ، $\tau(n)=\prod_{i=1}^{r}(e_i+1)$. إذاً

$$\tau(120)=(3+1)(1+1)(1+1)=16$$

وحيث أن $\sigma(n)=\prod_{i=1}^{r}\frac{p_i^{e_i+1}-1}{p_i-1}$. إذاً

$$\sigma(120)=\frac{2^4-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}=17\cdot4\cdot6=408$$

مثال (٣) :

أوجد أصغر عدد صحيح موجب n بحيث أن $\tau(n)=10$.

الحل :

بما أن $10=10\cdot1=5\cdot2$ ، إذاً $\tau(n)=(e_1+1)(e_2+1)=10\cdot1$ ، وعليه فإن $e_1=9\,,\,e_2=0 \vee e_1=4\,,\,e_2=1$. لكن $2^4\cdot3<2^9$. إذاً أصغر عدد صحيح هو $n=2^4\cdot3=48$.

وأخيراً إلى الدالة العددية $\sigma_m(n)$ والتي تعمم الدالتين $\tau(n)\,,\sigma(n)$.

تعريف ٤-٢-٢ :

$$\sigma_m(n)=\sum_{d\backslash n}d^m$$

مثال (٤) :

(أ) $\sigma_2(6)=1^2+2^2+3^2+6^2=50$.

(ب) $\sigma_3(10)=1^3+2^3+5^3+10^3=1134$.

لاحظ أن $\sigma_0(n)=\sum_{d\backslash n}1=\tau(n)$ ، $\sigma_1(n)=\sum_{d\backslash n}d=\sigma(n)$

مبرهنة ٤-٢-٤ :

(أ) $\sigma_m(n)$ دالة ضربية .

(ب) إذا كان $n=\prod_{i=1}^{r}p_i^{e_i}$ ، فإن $\sigma_m(n)=\prod_{i=1}^{r}\frac{p_i^{m(e_i+1)}-1}{p_i^m-1}$.

البرهان :

(أ) لتكن $f(a)=a^r$ لكل $a\in Z^+$. إذاً f دالة ضربية ، وعليه فإن $\sigma_m(n)=\sum_{d\backslash n}f(d)=\sum_{d\backslash n}d^m$ دالة ضربية حسب مبرهنة (٤-١-٣) .

(ب) بما أن $n=\prod_{i=1}^{r}p_i^{e_i}$. إذاً قواسم n هي $d=\prod_{i=1}^{r}p_i^{\alpha_i}$ حيث $0\le\alpha_i\le e_i$ ،

وعليه فإن

$$\sigma_m(n)=\sum_{\alpha_1=0}^{e_1}\sum_{\alpha_2=0}^{e_2}\cdots\sum_{\alpha_r=0}^{e_r}\left(\prod_{i=1}^{r}p_i^{m\alpha_i}\right)$$

$$=\prod_{i=1}^{r}\left(1+p_i^m+\cdots+p_i^{me_i}\right)$$

لكن $1,p_i^m,p_i^{2m},\cdots,p_i^{me_i}$ متوالية هندسية حدها الأول واحد وأساسها p_i^m

وعليه فإن مجموعها $S=\frac{p_i^{(e_i+1)m}-1}{p_i^m-1}$. إذاً $\sigma_m(n)=\prod_{i=1}^{r}\frac{p_i^{(e_i+1)m}-1}{p_i^m-1}$

□

مثال (٥) :

أحسب بإستخدام مبرهنة (٤-٢-٤) $\sigma(60)$ ، $\sigma(360)$.

الحل :

(أ) $60=2^2\cdot3\cdot5$. إذاً $p_1=2\ ,\ p_2=3\ ,\ p_3=5$ ،

$e_1=2\ ,\ e_2=1\ ,\ e_3=1$. لكن

$$\sigma(60)=\sigma_1(60)=\prod_{i=1}^{3}(1+p_i+p_i^2+\cdots+p_i^{e_i})$$

$$=(1+p_1+p_2^2)\,(1+p_2)\,(1+p_3)$$

$$=(1+2+2^2)\,(1+3)\,(1+5)=7\times4\times6=168$$

(ب) $360=2^3\cdot3^2\cdot5$. إذاً $e_1=3\ ,e_2=2\ ,e_3=1$ ،

$p_1=2\ ,\ p_2=3\ ,\ p_3=5$. لكن

$$\sigma(360)=\sigma_1(360)=(1+2+2^2+2^3)\,(1+3+3^2)\,(1+5)$$

$$=15\times13\times6=1170$$

تمـــــارين

(١) أحسب $\tau(n)$ ، $\sigma(n)$ لكل من $28,32,220,496,945$.

(٢) أحسب $\sigma(n)=\sigma_1(n)$ ، $\sigma_2(n)$ لكل من $192,600$.

(٣) أثبت أن $\sigma(n)=\sigma(n+1)$ عندما $n=206\,,957$.

(٤) إذا كان $n=14$ ، فأثبت أن $\sigma(n)=\sigma(n+1)$ ، $\tau(n)=\tau(n+1)$.

(٥) أوجد أصغر عدد صحيح موجب يحقق العلاقة $\tau(n)=6$.

(٦) إذا كان $n=2^{m-1}$ ، $m\geq 2$ ، فأثبت أن $\sigma(n)=2n-1$.

(٧) إذا كان $n=2^{m-1}(2^m-3)$ وكـــان 2^m-3 عـــدداً أوليـــاً ، $m>2$ ، فأثبت أن $\sigma(n)=2n+2$.

(٨) أثبت أن $\dfrac{\sigma(n)}{n}=\sum\limits_{d\backslash n}\dfrac{1}{d}$ ، ثم حقق ذلك عندما $n=14$ ، $n=36$.

(٩) إذا كان $n>1$ ، فأثبت أن $\prod\limits_{d\backslash n} d = n^{\frac{\tau(n)}{2}}$ ، ثم حقق ذلك عندما $n=12$.

(١٠) "الفارسي" إذا كانت $\sigma^*(n)$ تساوي مجموع أجــزاء أو القواســم الفعليــة للعدد n ، وكـــان $n=ab$ ، $(a,b)=1$ ، b عـــدداً أوليـــاً ، فأثبــت أن $\sigma^*(ab)=b\sigma^*(a)+\sigma^*(a)+a$ ، ثم أحسب $\sigma^*(84)$ ، $\sigma^*(284)$.

(١١) "الفارســــــي" إذا كــــــان $n=ab$ ، $(a,b)=1$ ، فأثبــــــت أن $\sigma^*(ab)=a\sigma^*(b)+b\sigma^*(a)+\sigma^*(a)\cdot\sigma^*(b)$ ، ثـــــم أحـــــسب $\sigma^*(60)$ ، $\sigma^*(84)$.

٤-٣ : " دالة أويلر Euler phi function "

عرّفنا دالة أويلر $\phi : Z^{+} \rightarrow Z^{+}$ كالآتي :

$$\phi(n) = \left| \left\{ a \in Z^{+} \,\middle|\, 1 \leq a \leq n \,,\, (a,n) = 1 \right\} \right|$$

وسنركز أهتمامنا في هذا الجزء على دراسة خواص تلك الدالة وبعض تطبيقاتها . لاحظ أن $\phi(n) = \sum\limits_{\substack{(a,n)=1 \\ 1 \leq a \leq n}} 1$

مبرهنة ٤-٣-١ :

إذا كان $n > 1$ ، فإن $\phi(n) = n - 1$ إذاً وإذا فقط كان n عدداً أولياً .

البرهان :

نفرض أن n عدد أولي . إذاً $1, 2, \cdots, n-1$ أعداد أولية نسبياً مع n ، وعليه فإن $\phi(n) = \left| \{ 1, 2, \cdots, n-1 \} \right| = n$.

ولإثبات العكس نفرض أن $\phi(n) = n - 1$ ، لكن n عدد مؤلف . إذاً $n = ab$ ، $1 < a < n$ ، $1 < b < n$ حسب مبرهنة (٢-٢-١) ، وعليه فإن $(n,a) = a \neq 1$ ، $(n,b) = b \neq 1$. إذاً يوجد على الأقل عددين من بين الأعداد $1, \cdots, n-1$ ليسا نسبيان أولياً مع n ، وعليه فإن $\phi(n) \leq n - 2$ وهذا يناقض الفرض . إذاً n عدد أولي .

□

مبرهنة ٤-٣-٢ :

إذا كان p عدداً أولياً ، فإن $\phi(p)^{m} = p^{m} - p^{m-1}$.

البرهان :

لتكن $A = \{1, 2, \cdots, p^{m}\}$. إذاً $|A| = p^{m}$. ولحساب $\phi(p)^{m} = \left| \{ a \in A \mid (a, p^{m}) = 1 \} \right|$ ،نفرض أن $B = \{ b \in A \mid (b, p^{m}) = d \neq 1 \}$ إذاً d عامل من عوامل p^{m} ، وعليه فإن $p \backslash d$ وهذا يعني وجود $r \in Z^{+}$ بحيث أن $d = pr$ ، لكن $p \leq b \leq p^{m}$. إذاً $p \leq rp \leq p^{m}$ ، وعليه فإن $1 \leq r \leq p^{m-1}$. إذاً $B = \{ p, 2p, 3p, \cdots, rp, \cdots, p^{m-1} \cdot p \}$ ، وعليه فإن $|B| = p^{m-1}$ ، وبالتالي فإن $\phi(p^{m}) = p^{m} - p^{m-1}$.

مثال (١) :

(أ) $\phi(2^5)=2^5-2^4=16$.

(ب) $\phi(3^4)=3^4-3^3=3^3(3-1)=3^3\cdot 2=24$.

ولحساب $\phi(n)$ لأي عدد طبيعي n ، نورد ما يلي .

مبرهنة ٤-٣-٣ :

ϕ دالة ضربية .

البرهان :

نفرض أن $m,n\in Z^+$ ، $(m,n)=1$ ، ولنفرض أن $f:Z^*_{mn}\to Z^*_m\times Z^*_n$ دالة معرفة كالآتي :

$f(b)=\big(b(\text{mod } m)\,,\,b(\text{mod } n)\big)$ لكل $b\in Z^*_{mn}=\{1,2,\cdots,mn-1\}$ ، $Z^*_m=\{1,2,\cdots,m-1\}$ ، $Z^*_n=\{1,2,\cdots,n-1\}$. إذاً f دالة متباينة (أحادية) ، لأن $f(b)=f(c)$ يعني أن $m\setminus b-c$ و $n\setminus b-c$. لكن $(m,n)=1$. إذاً $mn\setminus b-c$ حسب نتيجة (٢) مبرهنة (٢-١-٨) ، وعليه فإن $b\equiv c \text{ mod } (mn)$ وهذا يعني أن $b=c\in Z^*_{mn}$.

f دالة شاملة لأن لكل $(a,c)\in Z^*_m\times Z^*_n$ ، $(a,m)=1$ ، $(c,n)=1$ يوجد $b\in Z$ بحيث أن $b\equiv a\ (\text{mod } m)$ ، $b\equiv c\ (\text{mod } n)$ حسب مبرهنة الباقي الصينية . لكن $(b,m)=(a,m)=1$ ، $(b,n)=(c,n)=1$ ، إذاً $(b,mn)=1$ ، وعليه فإن $f(b)=(a,c)$ ، $b\in Z^*_{mn}$ ، إذاً f تقابل .

وعليه فإن $|Z^*_{mn}|=|Z^*_m|\times|Z^*_n|$ ، وبالتالي فإن $\phi(mn)=\phi(m)\cdot\phi(n)$.

□

نتيجة (١) :

إذا كان $n_1,\cdots,n_r\in Z^+$ ، $(n_i,n_j)=1$ لكل $i\neq j$ ، فإن

$$\phi\left(\prod_{i=1}^{r} n_i\right)=\prod_{i=1}^{r}\phi(n_i)$$

البرهان :

بالإستقراء على r ويترك للقارئ .

□

نتيجة (٢) :

إذا كان $n=\prod_{i=1}^{r} p_i^{e_i}$ ، فإن $\phi(n)=n\prod_{i=1}^{r}(1-\frac{1}{p_i})$.

البرهان :

إذا كان $r=1$ ، فإن $n=p_1^{e_1}$ ، وعليه فـإن $\phi(n)=p_1^{e_1}-p_1^{e_1-1}$ حسب مبرهنة (٤-٣-٢) . إذاً $\phi(n)=p_1^{e_1}(1-p_1^{-1})=p_1^{e_1}(1-\frac{1}{p_1})=n(1-\frac{1}{p_1})$

وعليه فإن النتيجة صحيحة عندما $r=1$. أما إذا كان $r\geq 2$ ، فإن $(p_i^{e_i}\ ,p_j^{e_i})=1$ لكل $i\neq j$ ، وعليه فإن

$$\phi(n)=\phi(\prod_{i=1}^{r}p_i^{e_i})=\prod_{i=1}^{r}\phi(p_i^{e_i})$$ " حسب نتيجة (١) "

$$=\prod_{i=1}^{r}(p_i^{e_i}-p_i^{e_i-1})$$ " حسب مبرهنة (٤-٣-٢) "

$$=\prod_{i=1}^{r}p_i^{e_i}(1-\frac{1}{p_i})=\prod_{i=1}^{r}p_i^{e_i}\cdot\prod_{i=1}^{r}(1-\frac{1}{p_i})$$

$$=n\cdot\prod_{i=1}^{r}(1-\frac{1}{p_i})$$

□

مثال (٢) :

أحسب $\phi(45)$ ، $\phi(192)$ ، $\phi(3600)$.

الحل :

(أ) بما أن $45=3^3\cdot 5$. إذاً

$$\phi(45)=\phi(3^3\cdot 5)=\phi(3^3)\cdot\phi(5)=3^2\cdot(1-\frac{1}{3})\cdot 4=3^2\cdot\frac{2}{3}\cdot 4=24$$

(ب) بما أن $192 = 2^6 \cdot 3$. إذاً

$$\phi(192) = \phi(2^6 \cdot 3) = \phi(2^6) \cdot \phi(3) = 2^6(1-\frac{1}{2}) \cdot 2 = 2^5 \cdot 2 = 2^6 = 64$$

(ج) بما أن $3600 = 3^2 \cdot 2^4 \cdot 5^2$. إذاً

$$\phi(3600) = \phi(3^2) \cdot \phi(2^4) \cdot \phi(5^2) = 3^2(1-\frac{1}{3}) \cdot 2^4(1-\frac{1}{2}) \cdot 5^2(1-\frac{1}{5})$$

$$= 3^2 \cdot \frac{2}{3} \cdot 2^4 \cdot \frac{1}{2} \cdot 5^2 \cdot \frac{4}{5} = 6 \cdot 8 \cdot 20 = 960$$

ملاحظة :

ϕ دالة ليست ضربية كلياً كما يوضح ذلك المثال الآتي

$$4 = \phi(12) = \phi(6 \cdot 2) \neq \phi(6) \cdot \phi(2) = 2 \cdot 1 = 2$$

والآن إلى خواص آخرى للدالة ϕ .

مبرهنة ٤-٣-٤ :

إذا كان $n > 2$ ، فإن $\phi(n)$ عدد زوجي .

البرهان :

إذا كان $n = 2^m$ ، $m \geq 2$ ، فإن $\phi(n) = \phi(2^m) = 2^m(1-\frac{1}{2}) = 2^{m-1}$ عدد زوجي . أما إذا كان $n \neq 2^m$ ، فإن $p \setminus n$ ، و p عدد أولي فردي ، وعليه يمكن أن يكون $n = ap^r$ ، $r \geq 1$ ، $(a,p^r) = 1$ ، وعليه فإن $\phi(n) = \phi(a) \cdot \phi(p^r) = p^{r-1}(p-1) \cdot \phi(a)$. لكن $2 \setminus p-1$ ، لأن p عدد أولي فردي ، إذاً $\phi(n)$ عدد زوجي .

□

مبرهنة ٤-٣-٥ :

إذا كان $n > 1$ ، وكان R نظام بواقي مختزل قياس n ، فإن $\sum_{a \in R} a = \frac{n}{2} \cdot \phi(n)$.

البرهان :

بما أن R نظام بواقي مختزل قياس n . إذاً $|R| = \phi(n)$ ، وعليه يمكن أن نفرض أن $R = \{a_1, \cdots, a_{\phi(n)}\}$ ، وبالتالي فإن $S = \sum_{a \in R} a = \sum_{a \in R}^{\phi(n)} a_i$. لكن $(a_i, n) = 1 \Leftrightarrow (n - a_i, n) = 1$. إذاً $S = \sum_{i=1}^{\phi(n)} (n - a_i)$ ، وعليه فإن

$$2S = \sum_{i=1}^{\phi(n)} a_i + \sum_{i=1}^{\phi(n)} (n - a_i) = \sum_{i=1}^{\phi(n)} n = n \cdot \phi(n)$$. إذاً $S = \frac{n}{2} \cdot \phi(n)$

□

مثال (٣) :

حقق مبرهنة (٤-٣-٥) عندما $n = 12$.

الحل :

بما أن $\phi(12) = 12(1 - \frac{1}{2})(1 - \frac{1}{3}) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$. إذاً توجد أربعة أعداد أقل من 12 وقاسمها المشترك الأعظم مع 12 يساوي واحد وهي 1,5,7,11 ، وعليه فإن

$$S = 1 + 5 + 7 + 11 = 24 \ , \ \frac{n}{2} \cdot \phi(n) = \frac{12}{2} \cdot \phi(12) = 24$$

وبالتالي فإن $S = \frac{n}{2} \cdot \phi(n)$.

مبرهنة ٤-٣-٦ :

إذا كان $n \in Z^+$ ، فإن $\sum_{d \backslash n} \phi(d) = n$.

البرهان :

لتكن $n = \prod_{i=1}^{r} p_i^{e_i}$. سنبرهن بالأستقراء على r أن $\sum_{d \backslash n} \phi(d) = n$. إذا كان $r = 1$ ، فإن $n = p_1^{e_1}$ ، وعليه فإن قواسم n هي $1, p_1, p_1^2, \cdots, p_1^{e_1}$

إذاً

$$\sum_{d\backslash n}\phi(d)=\phi(1)+\phi(p_1)+\phi(p_1^2)+\cdots+\phi(p_1^{e_1})$$

$$=1+(p_1-1)+p_1(p_1-1)+\cdots+p_1^{e_1-1}(p_1-1)$$

$$=1+(p_1-1)\left[1+p_1+\cdots+p_1^{e_1-1}\right]=1+(p_1-1)\cdot\frac{p_1^{e_1}-1}{p_1-1}$$

$$=p_1^{e_1}$$

وعليه فإن المبرهنة صحيحة عندما $r=1$. والآن لنفرض أن المبرهنة صحيحة عندما $r=m$. إذاً $n=\prod_{i=1}^{m}p_i^{e_i}\Rightarrow\sum_{d\backslash n}\phi(d)=n$.

ولإثبات صحة المبرهنة عندما $r=m+1$. لاحظ أن

$$a=\prod_{i=1}^{m+1}p_i^{e_i}=(\prod_{i=1}^{m}p_i^{e_i})\cdot p_{m+1}^{e_{m+1}}=n\cdot p_{m+1}^{e_{m+1}}$$

فإذا فرضنا أن $p_{m+1}=p$ ، $e_{m+1}=t$ ، فإن $a=n\cdot p^t$ ، $(p,n)=1$ ، $(p^t,n)=1$ ، وعليه إذا كان d قاسماً للعدد n ، فإن كلاً من $d,dp,dp^2,\cdots,dp^t$ قاسم للعدد a ، وعليه فإن

$$\sum_{d\backslash a}\phi(d)=\sum_{d\backslash n}\phi(n)+\sum_{d\backslash n}\phi(p^2d)+\cdots+\sum_{d\backslash n}\phi(dp^t)$$

لكن $(p^t,n)=1$, ϕ دالة ضربية . إذاً

$$\sum_{d\backslash a}\phi(d)=\sum_{d\backslash n}\phi(d)\left[1+\phi(p)+\cdots+\phi(p^t)\right]$$

$$=\sum_{d\backslash n}\phi(d)\cdot\sum_{b\backslash p^t}\phi(b)=n\cdot p^t=a$$

وعليه فإن المبرهنة صحيحة عندما $r=m+1$. إذاً المبرهنة صحيحة لكل $r\geq 1$.

□

<u>مثال (٤) :</u>

حقق مبرهنة (٤-٣-٦) عندما $n=3^2\cdot 5$.

الحل :

بما أن $\tau(n)=3\cdot 2=6$. إذاً كل من $1,3,3^2,5,15,45$ قاسم للعدد n ، وعليه فإن

$$\sum_{d\backslash n}\phi(d)=\phi(1)+\phi(3)+\phi(3^2)+\phi(5)+\phi(15)+\phi(45)$$

$$=1+2+3^2(1-\frac{1}{3})+4+\phi(3)\cdot\phi(5)+\phi(3^2)\cdot\phi(5)$$

$$=1+2+6+4+2(4)+6(4)=13+8+24=45=n$$

□

ملاحظة (١) :

لحل المعادلة $\phi(x)=m$ ، لاحظ أن :

$$x=\prod_{i=1}^{r}p_i^{e_i}\Rightarrow\phi(x)=\prod_{i=1}^{r}(p_i^{e_i}-p_i^{e_i-1})=\prod_{i=1}^{r}p_i^{e_i-1}(p_i-1)m$$

إذاً إذا كان $d_i=p_i-1$ ، $i=1,\cdots,r$ ، فإن

$$\prod_{i=1}^{r}p_i^{e_i-1}d_i=m\Rightarrow\prod_{i=1}^{r}(\frac{p_i^{e_i}}{p_i})d_i=m\Rightarrow\prod_{i=1}^{r}p_i^{e_i}(\frac{d_i}{p_i})=m$$

$$\Rightarrow(\prod_{i=1}^{r}p_i^{e_i})\cdot\prod_{i=1}^{r}(\frac{d_i}{p_i})=m\Rightarrow x\cdot\prod_{i=1}^{r}p_i^{e_i}(\frac{d_i}{p_i})=m\Rightarrow x=\frac{m}{\prod_{i=1}^{r}d_i}\cdot\prod_{i=1}^{r}p_i$$

وعليه فإن لحل المعادلة $\phi(x)=m$ ، نوجد d_i بحيث أن $d_i\backslash m$ و (d_i+1) عدد أولي . كما أن $\frac{m}{\prod_{i=1}^{r}d_i}$ عدد صحيح موجب لا يحوي أي قاسم أولي غير موجود في $\prod_{i=1}^{r}p_i$.

ولتوضيح هذه الطريقة نورد الأمثلة الآتية :

مثال (٥) :

حل المعادلة $\phi(x)=12$.

الحل :

بما أن قواسم العدد $12 = 2^2 \cdot 3$ هي $1,2,3,4,6,12$. إذاً $d \backslash 12$ و $d+1$ عدد أولي يعني أن $d \in \{1,2,3,4,6,12\}$. وبتطبيق الشروط أعلاه نجد أن

$\prod_{i=1}^{r} d_i$	$\frac{6}{\prod_{i=1}^{r} d_i}$	$\prod_{i=1}^{r} p_i$	$x = \frac{6}{\prod_{i=1}^{r} d_i} \cdot \prod_{i=1}^{r} p_i$
$1 \cdot 2$	$2 \cdot 3$	$2 \cdot 3$	$2^2 \cdot 3^2 = 36$
$1 \cdot 6$	2	$2 \cdot 7$	$2^2 \cdot 7 = 28$
$1 \cdot 12$	1	$2 \cdot 13$	$1 \cdot 2 \cdot 13 = 26$
12	1	13	$1 \cdot 13 = 13$
$2 \cdot 6$	1	$3 \cdot 7$	$3 \cdot 7 = 21$
$1 \cdot 2 \cdot 6$	1	$2 \cdot 3 \cdot 7$	$2 \cdot 3 \cdot 7 = 42$

إذاً مجموعة حل المعادلة $\phi(x) = 12$ هي $\{13,21,26,28,36,42\}$.

مثال (٦) :

حل المعادلة $\phi(x) = 6$.

الحل :

بما أن قواسم العدد 6 هي $1,2,3,6$. إذاً $d \backslash 6$ و $d+1$ عدد أولي يعني أن $d \in \{1,2,6\}$ وبتطبيق الشرط $\frac{6}{\prod_{i=1}^{r} d_i}$ عدد صحيح موجب لا يحوي أي قاسم أولي غير موجود في $\prod_{i=1}^{r} p_i$ نجد أن

$\prod_{i=1}^{r} d_i$	$\frac{6}{\prod_{i=1}^{r} d_i}$	$\prod_{i=1}^{r} p_i$	$x = \frac{6}{\prod_{i=1}^{r} d_i} \cdot \prod_{i=1}^{r} p_i$
2	3	3	$3 \cdot 3 = 9$
6	1	7	$1 \cdot 7 = 7$
$1 \cdot 2$	3	$2 \cdot 3$	$2 \cdot 3^2 = 18$
$1 \cdot 6$	1	$2 \cdot 7$	$1 \cdot 2 \cdot 7 = 14$

وعليه فإن مجموعة الحل هي $\{9,7,14,18\}$.

ملاحظة (٢) :

إذا كان عدد الحلول معلوماً أو أن m صغيرة ، فيمكن تطبيق مبرهنة (٤-٣-٣) لإيجاد عددين أوليين نسبياً a,b بحيث أن $\phi(x=ab)=\phi(a)\cdot\phi(b)=m$.

وبالرجوع إلى المثال (٦) ، لاحظ أن

$$(1,7)=1 \Rightarrow \phi(7)=\phi(1)\phi(7)=6 \Rightarrow x=7$$
$$(1,9)=1 \Rightarrow \phi(9)=6 \Rightarrow x=9$$
$$(2,7)=1 \Rightarrow \phi(14)=\phi(2)\cdot\phi(7)=1\cdot 6=6 \Rightarrow x=14$$
$$(2,9)=1 \Rightarrow \phi(18)=\phi(2)\cdot\phi(9)=1\cdot 6=6 \Rightarrow x=18$$

وعليه فإن مجموعة الحل هي $\{7,9,14,18\}$

مثال (٧) :

حل المعادلة $\phi(x)=10$.

الحل :

$$(1,11)=1 \Rightarrow \phi(1\cdot 11)=\phi(1)\cdot\phi(11)=1\cdot 10=10 \Rightarrow x=11$$
$$(2,11)=1 \Rightarrow \phi(2\cdot 11)=\phi(2)\cdot\phi(11)=1\cdot 10=10 \Rightarrow x=22$$

وعليه فإن مجموعة الحل هي $\{11,22\}$.

وبتطبيق الطريقة الواردة في الملاحظة (١) نحصل على نفس الجواب ، لأن قواسم العدد 10 هي $1,2,5,10$ و $d\backslash 10 \Leftrightarrow d+1$ عدد أولي يعني أن $d\in\{1,2,10\}$ ، وبالتالي فإن

$t=\prod_{i=1}^{r} d_i$	$\frac{10}{t}$	$\prod_{i=1}^{r} p_i$	$x=\frac{10}{t}\cdot\prod_{i=1}^{r} p_i$
10	1	11	11
$1\cdot 10$	1	$2\cdot 11$	22

تمـــــارين

(١) أحسب $\phi(n)$ عندما $n = 360 , 540 , 8316 , 245000$.

(٢) أوجد أصغر عدد أولي p بحيث أن $7 \backslash \phi(p)$.

(٣) إذا كان n عدداً فردياً ، فأثبت أن $\phi(2n) = \phi(n)$.

(٤) (أ) إذا كـــان p عـــدداً أوليـــاً ، $n \in Z^+$ وكـــان $p \backslash n$ ، فأثبـــت أن $p - 1 \backslash \phi(n)$.

(ب) بين بمثال على أن $p - 1 \backslash \phi(n)$ لا يعني أن $p \backslash n$.

(٥) إذا كان $n, d \in Z^+$ و $d \backslash n$ ، فأثبت أن $\phi(d) \backslash \phi(n)$.

(٦) إذا كان $n = \prod_{i=1}^{r} p_i^{e_i}$ ، فأثبت أن $\sum_{d \backslash n} d\phi(d) = \prod_{i=1}^{r} \frac{p^{2e_i+1} + 1}{p_i + 1}$.

(٧) حقق مبرهنة (٤-٣-٥) عندما $n = 48$.

(٨) حقق مبرهنة (٤-٣-٦) عندما $n = 78$ وعندما $n = 150$.

(٩) إذا كـــــان $d = (m, n)$ ، فأثبـــــت أن $\phi(mn) = \frac{d\phi(m) \cdot \phi(n)}{\phi(d)}$

ثم حقق ذلك عندما $m = 28$ ، $n = 42$.

(١٠) إذا كان n عدداً زوجياً ، فأثبت أن $\phi(2n) = 2\phi(n)$.

(١١) أثبت أن $\phi(n^2) = n\phi(n)$ ، ثـــم أثبـــت أن $\phi(n^m) = n^{m-1}\phi(n)$ لكـــل $m \geq 2$.

(١٢) إذا كان $m, n \in Z^+$ و $m\phi(m) = n\phi(n)$ ، فأثبت أن $m = n$.

(١٣) حل المعادلة $\phi(x) = m$ عندما $m = 4 , m = 16 , m = 24 , m = 72$

(١٤) إذا كان p عدداً أولياً وكان $2p+1$ عدداً مؤلفاً ، فبرهن على عدم وجود حل للمعالة $\phi(x)=2p$.

(١٥) برهن على عدم وجود حل لكل مما يأتي :

$\phi(x)=26$ ، $\phi(x)=34$ ، $\phi(x)=124$.

٤-٤ : دالة موبيص " The Möbius function $\mu(n)$ "

ظهرت الدالة $\mu(n)$ بصورة غير مباشرة في أعمال أويلر سنة ١٧٤٨م لكن الألماني موبيص (١٧٩٠-١٨٦٨) هو أول من درس خواصها سنة ١٨٣٢م . وسنركز أهتمامنا في هذا الجزء على تعريف هذه الدالة ودراسة خواصها وعلاقتها بالدوال العددية الأخرى .

تعريف ٤-٤-١ :

إذا كان $n\in Z^{+}$ ، فتعرف $\mu(n)$ كالآتي :

$$\mu(n)=\begin{cases}1 & \text{إذا كان } n=1\\ 0 & \text{إذا كان } p \text{ عدداً أولياً }, p^2 b\\ (-1)^r & \text{إذا كان } n=\prod_{i=1}^{r} p_i \text{ و } p_i \text{ أعداد أولية مختلفة}\end{cases}$$

مثال (١) :

(أ) $\mu(1)=1\ ,\ \mu(2)=-1\ ,\ \mu(10)=(-1)^2=1\ ,\ \mu(16)=0$.

(ب) إذا كان p عدداً أولياً ، فإن $\mu(p)=-1$ و $\mu(p^m)=0$ لكل $m\geq 2$.

والآن إلى دارسة خواص دالة موبيص .

مبرهنة ٤-٤-١:

μ دالة ضربية .

البرهان :

نفرض أن $a,b\in Z^{+}$ ، $(a,b)=1$. إذاً :

(أ) إذا كان $a=1$ أو $b=1$ ، يمكننا أن نفرض أن $b=1$ فنجد أن $\mu(ab)=\mu(a)=\mu(a)\cdot 1=\mu(a)\cdot\mu(b)$.

(ب) إذا كان p عدداً أولياً و $p^2 \backslash a$ أو $p^2 \backslash b$، فإن $p^2 \backslash ab$ كما أن $\mu(a)=0$ أو $\mu(b)=0$ ، وعليه فإن $\mu(ab)=0=\mu(a)\cdot\mu(b)$.

(ج) إذا كان $p^2 \nmid a$ أو $p^2 \nmid b$ و p عدد أولي ، فإن $a=\prod_{i=1}^{r} p_i , b=\prod_{j=1}^{s} q_j$

حيث p_i , q_j أعداد أولية مختلفة ، إذاً

$$\mu(ab)=\mu(p_1p_2\cdots p_r\cdot q_1q_2\cdots q_2)=(-1)^{r+2}$$
$$=(-1)^r\cdot(-1)^s=\mu(a)\cdot\mu(b)$$

□

مثال (٢) :

ليكن $n=30$. إذاً $n=2\cdot3\cdot5$ ، وعليه فإن قواسم n هي $1,2,3,5,6,10,15,30$ ، وبالتالي فإن

$$\sum_{d\backslash 30}\mu(d)=\mu(1)+\mu(2)+\mu(5)+\mu(6)+\mu(10)+\mu(15)+\mu(30)$$
$$=1+(-1)+(-1)+(-1)+1+1+1+(-1)=4-4=0$$

وبصورة عامة يمكن أن نبرهن ما يلي :

مبرهنة ٤-٤-٢ :

إذا كان $n\geq 1$ ، فإن

$$\sum_{d\backslash n}\mu(d)=\begin{cases}1 & \text{عندما } n=1\\ 0 & \text{عندما } n>1\end{cases}$$

البرهان :

لتكن $F(n)=\sum_{d\backslash n}\mu(d)$. إذاً $F(1)=\sum_{d\backslash 1}\mu(d)=\mu(1)=1$

وإذا كان $n=p^m$ حيث p عدد أولي ، فإن

$$F(p^m)=\sum_{d\backslash p^m}\mu(d)=\mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^m)$$

لكن $\mu(p^m)=0$ لكل $m\geq 2$ ، $\mu(p)=-1$ ، $\mu(1)=1$.

إذاً $F(p^m)=1-1=0$.

والآن لنفرض أن $n=\prod_{i=1}^{r} p_i^{e_i}$. إذاً $F(n)=F(\prod_{i=1}^{r} p_i^{e_i})$. لكن F دالة ضربية

حسب مبرهنة (٤-١-٣) ، إذاً $F(n)=\prod_{i=1}^{r} p_i^{e_i} F(p_i^{e_i})=0$ ، وعليه فإن

$$\sum_{d\backslash n}\mu(d)=\begin{cases}1 & n=1 \text{ عندما} \\ 0 & n>1 \text{ عندما}\end{cases}$$

□

مبرهنة ٤-٤-٣ :

إذا كان $n=\prod_{i=1}^{r} p_i^{e_i}$ وكانت f دالة ضربية ، فإن

$$\sum_{d\backslash n}\mu(d)f(d)=\prod_{i=1}^{r}\left(1-f(p_i)\right)$$

البرهان :

نفرض أن $g(n)=\sum_{d\backslash n}\mu(d)f(d)$. إذاً g دالة ضربية حسب مبرهنة (٤-١-٣)

وعليه فإن $g(n)=g(\prod_{i=1}^{r} p_i^{e_i})=\prod_{i=1}^{r} g(p_i^{e_i})$. لكن

$$g(p_i^{e_i})=\sum_{d\backslash p_i^{e_i}}\mu(d)f(d)$$

$$=\mu(1)f(1)+\mu(p_i)f(p_i)+\mu(p_i^2)f(p_i^2)+\cdots+\mu(p_i^{e_i})f(p_i^{e_i})$$

لكن f دالة ضربية ، إذاً $(f)=1$ كما أن $\mu(1)=1$ ، $\mu(p_i)=-1$ ،

$\mu(p_i^{e_i})=0$ لكل $e_i\geq 2$ ، وعليه فإن $g(p_i^{e_i})=1-f(p_i)$ ، وبالتالي فإن

$$g(n)=\sum_{d\backslash n}\mu(d)\,f(d)=\prod_{i=1}^{r} g(p_i^{e_i})=\prod_{i=1}^{r}\left(1-f(p_i)\right)$$

مبرهنة ٤-٤-٤ : " قانون التعاكس لموبيص Möbus Inversion formula "

إذا كانت f،g دالتين عدديتين وكانت $g(n)=\sum_{d\backslash n} f(d)$ ، فإن

$$f(n)=\sum_{d\backslash n}\mu(d)g(\frac{n}{d})=\sum_{d\backslash n}\mu(\frac{n}{d})\,g(d)$$

البرهان :

$$\sum_{d\backslash n}\mu(d)\,g(\frac{n}{d})=\sum_{d\backslash n}\mu(d)\cdot\sum_{b\backslash\frac{n}{d}}f(b)=\sum_{d\backslash n}\left(\sum_{b\backslash\frac{n}{d}}\mu(d)\,f(b)\right)$$

لكن $d\backslash n$ و $b\backslash(\frac{n}{d}) \Leftrightarrow b\backslash n$ و $d\backslash(\frac{n}{d})$. إذاً

$$\sum_{d\backslash n}\mu(d)\,g(\frac{n}{d})=\sum_{b\backslash n}\left(\sum_{d\backslash(\frac{n}{b})}f(b)\cdot\mu(d)\right)=\sum_{b\backslash n}f(b)\cdot\sum_{d\backslash\frac{n}{b}}\mu(d)$$

لكن $\sum_{d\backslash\frac{n}{b}}\mu(d)=0$ لكل $\frac{n}{b}\neq 1$ و $\sum_{d\backslash\frac{n}{b}}\mu(d)=1$ عندما $\frac{n}{b}=1$

حسب مبرهنة (٤-٤-٢) . إذاً

$$\sum_{d\backslash n}\mu(d)g(\frac{n}{d})=\sum_{b=n}f(b)\cdot 1=\sum_{b=n}f(b)=f(n)$$

وحيث أن $\sum_{d\backslash n}\mu(d)g(\frac{n}{d})=\sum_{d\backslash n}\mu(\frac{n}{d})g(d)$ لأنه إذا كان d قاسماً للعدد n فإن $\frac{n}{d}$ قاسم للعدد n أيضاً وعدد القواسم d يساوي عدد القواسم $\frac{n}{d}$. إذاً

$$f(n)=\sum_{d\backslash n}\mu(d)g(\frac{n}{d})=\sum_{d\backslash n}\mu(\frac{n}{d})g(d)$$

□

نتيجة (١) :

(أ) $\sum_{d\backslash n}\mu(\frac{n}{d})\tau(d)=1$ ، (ب) $\sum_{d\backslash n}\mu(\frac{n}{d})\sigma(d)=n$

(ج) $\frac{\phi(n)}{n}=\sum_{d\backslash n}\frac{\mu(d)}{d}$.

<u>البرهان :</u>

(أ) بمـــا أن $\tau(n)=\sum_{d\backslash n} 1$. إذاً $\sum_{d\backslash n}\mu(d)\,\tau(\frac{n}{d})=\sum_{d\backslash n}\mu(\frac{n}{d})\tau(d)=1$ حـــسب قانون موبيص للتعاكس .

(ب) بمـــــا أن $\sigma(n)=\sum_{d\backslash n} d$. إذاً $\sum_{d\backslash n}\mu(\frac{n}{d})\,\sigma(d)=\sum_{d\backslash n}\mu(d)\,\sigma(\frac{n}{d})=n$ حسب قانون موبيص للتعاكس .

(ج) بمـــا أن $n=\sum_{d\backslash n}\phi(d)=\sum_{d\backslash n}\phi(\frac{n}{d})$ حـــسب مبرهنـــة (٤-٣-٦) . إذاً $\phi(n)=\sum_{d\backslash n}\mu(d)\cdot\frac{n}{d}$ حسب قـانون مـوبيص للتعـاكس ، وعليـه فـإن $\frac{\phi(n)}{n}=\sum_{d\backslash n}\frac{\mu(d)}{d}$.

□

<u>نتيجة (٢)</u> : " عكس مبرهنة ٤-١-٣ "

إذا كانت g دالة ضربية و $g(n)=\sum_{d\backslash n} f(d)$ ، فإن f دالة ضربية .

<u>البرهان :</u>

ليكن $a,b\in\mathbb{Z}^+$ و $(a,b)=1$. إذاً $f(ab)=\sum_{d\backslash ab}\mu(d)g(\frac{ab}{d})$ حسب قـانون موبيص للتعاكس لكن $d\backslash ab$. إذاً وإذا فقط وجد عـددان وحيـدان $c,e\in\mathbb{Z}^+$ بحيث أن $c\backslash a$ و $e\backslash b$ ، $(c,e)=1$ ، $d=ce$ حسب مبرهنـة (٢-٣-٢) .

إذاً $f(ab)=\sum_{\substack{d\backslash a\\ e\backslash b}}\mu(ce)g(\frac{ab}{ce})$.

لكن كلاً من μ,g دالة ضربية . إذاً

$$f(ab)=\sum_{\substack{c\backslash a\\ e\backslash b}}\mu(c)\mu(e)g(\frac{a}{c})\cdot g(\frac{b}{e})=\sum_{c\backslash a}\mu(c)\,g(\frac{a}{c})\cdot\sum_{e\backslash b}\mu(e)g(\frac{b}{e})=f(a)\cdot f(b)$$

وعليه فإن f دالة ضربية .

تمـــــارين

(١) أحسب $\mu(n)$ عندما $n = 18 , 23 , 34, 35, 48, 90$.

(٢) أوجد $n \in \mathbb{Z}^+$ بحيث أن $\mu(n) + \mu(n+1) + \mu(n+2) = 3$.

(٣) أثبت أن $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) =$ لكل $n \in \mathbb{Z}^+$.

(٤) أثبت أن $\sum_{k=1}^{n} \mu(k!) = 1$ لكل $n \geq 3$.

(٥) إذا كـــان $n = \prod_{i=1}^{r} p_i^{e_i}$ ، فأثبـــت بتطبيـــق مبرهنـــة (٤-٤-٣) أن :

(أ) $\sum_{d\backslash n} \mu(d)\, \tau(d) = (-1)^r$ ، (ب) $\sum_{d\backslash n} \mu(d)\, \sigma(d) = (-1)^r \prod_{i=1}^{r} p_i$

(ج) $\sum_{d\backslash n} \frac{\mu(d)}{d} = \prod_{i=1}^{r} p_i (1 - \frac{1}{p_i})$ ، (د) $\sum_{d\backslash n} d\,\mu(d) = \prod_{i=1}^{r} (1 - p_i)$

(هـ) حقق " أ ، ب ، ج ، د " عندما $n = 2^3 \cdot 3^5 \cdot 7^2$.

(٦) إذا كان

$$\wedge(n) = \begin{cases} \ln p & p \text{ عدداً أولياً}, m \geq 1 \\ 0 & n \neq p^m \end{cases}$$

، فأثبت أن

$\wedge(n) = \sum_{d\backslash n} \mu\left(\frac{n}{d}\right) \ln(d) = -\sum_{d\backslash n} \mu(d) \ln(d)$. تسمى هذه الدالة دالة $\wedge$

مانجولد " لاحظ أن $\sum_{d\backslash n} \wedge(d) = \ln(n)$ وبتطبيق قانون موبيص للتعاكس

تحصل على المطلوب " .

(٧) أثبت أن $f(n) = n\mu(n)$ دالة ضربية ، ثم أثبت أن

$\sum_{d\backslash n} d\,\mu(d) = \frac{(-1)^r \phi(n) \prod_{i=1}^{r} p_i}{n}$ ، ثم حقق ذلك عندما $n = 40500$.

(٨) إذا كانت λ دالة ليوفيلي ، فأثبت أن $\sum_{d\backslash n} \mu(d)\, \lambda(d) = 2^r$.

٤-٥ : الدالة زيتا $\zeta(s)$ The Zeta function

عُرّفت $\zeta(s)$ من قبل أويلر سنة ١٧٣٧م لكل $s \in R^+$ ، ثم وسّع ريمان التعريف سنة ١٨٥٩م لكل $s \in C - \{1\}$ ، ولهذا تسمى هذه الدالة دالة زيتا الريمانية (Riemann Zeta function) وتمكن أهمية هذه الدالة في كثرة تطبيقاتها في نظرية الأعداد والفيزياء النظرية . وسنركز أهتمامنا في هذا الجزء على دراسة بعض الخواص الأساسية لهذه الدالة .

تعريف ٤-٥-١ :

إذا كان $s = a + ib \in C$ ، فتعرف الدالة زيتا كالآتي :

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ ، } R(s) = a > 0 .$$

مثال (١) : " أويلر "

$$\zeta(4) = \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90} \text{ ، } \zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

مبرهنة ٤-٥-١ : " أويلر "

إذا كان $R(s) > 1$ ، فإن $\zeta(s) = \prod_{p \in P} (1 - p^{-s})^{-1}$ ، حيث P مجموعة جميع الأعداد الأولية .

البرهان :

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots + \frac{1}{n^s} + \cdots$$

$$= (1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots)(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots)(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \cdots)\cdots$$

$$= \prod_{p \in P} (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots) = \prod_{p \in P} \sum_{m=0}^{\infty} p^{-ms}$$

لكـــن $p \geq 2$ و $R(s) > 1$. إذاً $\sum_{m=0}^{\infty} p^{-ms}$ متقاربـــة بـــصورة مطلقـــة و $\sum_{m=0}^{\infty} p^{-ms} = (1-p^{-s})^{-1}$ ، وعليه فإن $\zeta(s) = \prod_{p \in P} (1-p^{-s})^{-1}$.

□

ولحساب بعض قيم $\zeta(s)$ نورد الآتي .

تعريف ٤-٥-٢ :

تعرف أعداد برنولي(Bernoulli numbers)، B_m بالمعاملات في متسلسلة القوى

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{m=1}^{\infty} (-1)^{m+1} B_m \frac{x^{2m}}{(2m)!}$$

ومنها نجد أن

$$B_1 = \frac{1}{6} \;,\; B_2 = \frac{1}{30} \;,\; B_3 = \frac{1}{42} \;,\; B_4 = \frac{1}{30} \;,\; B_5 = \frac{5}{66}$$

$$B_6 = \frac{691}{2730} \;,\; B_7 = \frac{7}{6} \;,\; B_8 = \frac{3617}{510} \;,\; B_9 = \frac{43867}{798} \text{ ،}$$

$$B_{10} = \frac{283617}{330} \;,\; B_{11} = \frac{11131593}{138}$$

ملاحظة :

يمكن تعريف أعداد برنولي كالآتي $\frac{x}{e^x - 1} = \sum_{m=0}^{\infty} \frac{b_m x^m}{m!}$ ، ومنها نجد أن

$$b_0 = 1 \;,\; b_1 = -\frac{1}{2} \;,\; b_{2m+1} = 0 \;\forall m > 1 \;,\; b_{2m} = (1-)^{m-1} B_m$$

مبرهنة ٤-٥-٢ :

إذا كان m عدداً صحيحاً موجباً أكبر من الواحد ، فإن

$$\zeta(2m) = \frac{2^{2m-1}}{(2m)!} B_m \pi^{2m}$$

البرهان :

من تعريف أعداد برنولي ووضع $x = 2iz$ ، نجد أن

$$z \cot z = 1 - \sum_{m=1}^{\infty} B_m \frac{2^{2m} z^{2m}}{(2m)!} \qquad \dots (1)$$

لكن $\sin z = z \cdot \prod_{n=1}^{\infty}(1 - \frac{z^2}{n^2\pi^2})$. إذاً

$ln(\sin z) = ln(z) + \sum_{n=1}^{\infty} ln\,(1 - \frac{z^2}{n^2\pi^2})$ ، وعليه فإن

$\frac{1}{\sin z} \cdot \cos z = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{1}{(1 - \frac{z^2}{n^2\pi^2})} \cdot \frac{-2z}{n^2\pi^2}$ ، ومنها نجد أن

$$z\cot z = 1 + 2\sum_{n=1}^{\infty} \frac{z^2}{z^2 - n^2\pi^2} = 1 - 2\sum_{n=1}^{\infty} \frac{1}{(1 - \frac{z^2}{n^2\pi^2})} \cdot \frac{z^2}{n^2\pi^2}$$

$$= 1 - 2\sum_{n=1}^{\infty} (1 - \frac{z^2}{n^2\pi^2})^{-1} \cdot \frac{z^2}{n^2\pi^2} = 1 - 2\sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{z^{2m}}{n^{2m}\pi^{2m}} \quad \cdots(2)$$

ومن (1) ، (2) ينتج أن

$$\sum_{m=1}^{\infty} B_m \cdot \frac{2^{2m} \cdot z^{2m}}{(2m)!} = 2\sum_{n=1}^{\infty} \frac{1}{n^{2m}} \cdot \sum_{m=1}^{\infty} \frac{z^{2m}}{\pi^{2m}}$$

وعليه فإن

$$B_m \cdot \frac{2^{2m-1}}{(2m)!} \cdot \pi^{2m} = \sum_{n=1}^{\infty} \frac{1}{n^{2m}} = \zeta(2m)$$

□

مثال (٢) :

(أ) $\zeta(2) = B_1 \cdot \frac{2}{2!}\pi^2 = \pi^2 B_1 = \frac{\pi^2}{6}$.

(ب) $\zeta(4) = \frac{2^3}{4!}\pi^4 \cdot B_2 = \frac{\pi^4}{3} \cdot B_2 = \frac{\pi^4}{3} \cdot \frac{1}{30} = \frac{\pi^2}{90}$.

(ج) $\zeta(6) = \frac{2^5}{6!}\pi^6 \cdot B_3 = \frac{32\pi^6}{6!} \cdot \frac{1}{42} = \frac{\pi^6}{3^3 \cdot 5 \cdot 7} = \frac{\pi^6}{945}$.

مبرهنة ٤-٥-٣ :

إذا كان $R(s) > 0$ ، فإن $\zeta(s) = \frac{1}{1-2^{1-s}} \cdot \eta(s)$. حيث $\eta(s) = \sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$
تسمى $\eta(s)$ دالة ايتا الدركلية (Dirichlet eta function) نسبه للألماني ديركلي (١٨٠٥-١٨٥٩م) .

البرهان :

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s} + \sum_{n=1}^{\infty} \frac{1}{n^s} = 2 \sum_{n=2,4,\dots}^{\infty} \frac{1}{n^s} = 2\sum_{m=1}^{\infty} \frac{1}{(2m)^s}$$

$$= 2^{1-s} \cdot \sum_{m=1}^{\infty} \frac{1}{m^s}$$

وعليه فإن $\eta(s) + \zeta(s) = 2^{1-s} \cdot \zeta(s)$ ، ومنها نجد أن $\zeta s) = \frac{1}{1-2^{1-s}} \cdot \eta(s)$

□

مبرهنة ٤-٥-٤ :

$$\zeta(s) \sim \frac{1}{s-1}$$

" $\zeta(s) \sim \frac{1}{s-1}$ يعني $\lim_{s \to 1} (s-1)\zeta(s) = 1$ "

البرهان :

بما أن $(s-1)\zeta(s) = (1-2^{1-s})\zeta(s) \cdot \frac{s-1}{1-2^{1-s}}$. إذاً

$$\lim_{s \to 1} (s-1)\zeta(s) = \lim_{s \to 1} (1-2^{1-s})\zeta(s) \cdot \lim_{s \to 1} \frac{s-1}{1-2^{1-s}}$$

$$= \lim_{s \to 1} \sum \frac{(-1)^n}{n^s} \cdot \lim_{s \to 1} \frac{s-1}{1-2^{1-s}} = \ln 2 \cdot \frac{1}{\ln 2} = 1$$

وعليه فإن $\zeta(s) \sim \frac{1}{s-1}$

□

والآن إلى دراسة علاقة الدالة زيتا بالدوال العددية الأخرى .

مبرهنة ٤-٥-٥ :

إذا كان $R(s)>1$ فإن $\frac{1}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$

البرهان :

بما أن $\frac{1}{\zeta(s)}=\prod_{p\in P}(1-p^{-s})$ حسب مبرهنة (٤-٥-١)

$$=\prod_{p\in P}\left[1+\mu(p)p^{-s}+\mu(p^2)p^{-2s}+\cdots\right]$$

$$=\sum_{n=1}^{\infty}\mu(n)n^{-s}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$$

□

مبرهنة ٣-٥-٦ :

إذا كان $R(s)>2$ فإن $\frac{\zeta(s-1)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\phi(n)}{n^s}$

البرهان :

بما أن $\frac{\zeta(s-1)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{n}{n^s}\cdot\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$ حسب تعريف ζ ومبرهنة (٤-٥-٥)

إذاً $\frac{\zeta(s-1)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{1}{n^s}\cdot\sum_{d\backslash n}d\mu(\frac{n}{d})=\sum_{n=1}^{\infty}\frac{\phi(n)}{n^s}$

□

مبرهنة ٤-٥-٧ :

إذا كان $s\in R$ و $s>m+1$ ، فإن $\zeta(s)\zeta(s-m)=\sum_{n=1}^{\infty}\frac{\sigma_m(n)}{n^s}$

البرهان :

$$\zeta(s)\,\zeta(s-m)=\sum_{n=1}^{\infty}\frac{1}{n^s}\cdot\sum_{n=1}^{\infty}\frac{n^m}{n^s}$$

$$=\sum_{n=1}^{\infty}\frac{1}{s}\cdot\sum_{d\backslash n}d^m=\sum_{n=1}^{\infty}\frac{\sigma_m(n)}{n^s}$$

نتيجة (١) :

(أ) إذا كان $1 < s \in \mathbb{R}$ ، فإن $\zeta^2(s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$.

(ب) إذا كان $2 < s \in \mathbb{R}$ ، فإن $\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}$.

البرهان :

بما أن $\zeta(s)\zeta(s-m) = \sum_{n=1}^{\infty} \frac{\sigma_m(n)}{n^s}$ حسب مبرهنة (٤-٥-٧) .

إذاً عندما $m = 0$. نجد أن $\zeta^2(s) = \sum_{n=1}^{\infty} \frac{\sigma_0(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$

وعندما $m = 1$ ، نجد أن $\zeta(s) \cdot \zeta(s-1) = \sum_{n=1}^{\infty} \frac{\sigma_1(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}$.

□

تمـــــارين

(١) أحسب $\zeta(8)$ ، $\zeta(10)$ ، $\zeta(12)$.

(٢) أثبت أن

(أ) $\sum \frac{\mu(n)}{n^s} = \frac{6}{\pi^2}$ ، (ب) $\zeta^2(2) = \frac{\pi^4}{36}$

(ج) $\sum_{n=1}^{\infty} \frac{\sigma_4(n)}{n^2} = \zeta(2) \cdot \zeta(4) = \frac{\pi^6}{540}$.

(٣) إذا كان $s > 1$ ، فأثبت أن $\frac{\zeta(2s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{(-1)^m}{n^s}$ حيث m يساوي عدد العوامل الأولية في n .

" لاحظ أن $\frac{\zeta(2s)}{\zeta(s)} = \prod_{p \in P} (\frac{1-p^{-s}}{1-p^{-2s}}) = \prod_{p \in P} (1+p^{-s})^{-1}$ "

(٤) إذا كان $s > 1$ ، فأثبت أن $\frac{\zeta^4(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{\sigma^2(n)}{n^s}$.

الفصل الخامس

أعداد خاصة Special Numbers

سنركز اهتمامنا في هذا الفصل على دراسة أنواع معينة من الأعــداد هــي أعداد فيرما وأعداد مرسين ، الأعداد التامة والأعداد المتحابة والأعداد المتعادلة .

٥-١ : أعداد فيرما وأعداد مرسين Fermat and Mersenne Numbers

من أحدى طرق إيجاد أعداد أولية كبيرة هي دراسة الأعــداد التــي علــى الصورة $a^m - 1$ أو $a^m + 1$ ، وقد أثبتنا في مبرهنة (٢-٢-٦) ، أنه إذا كــان $a^m - 1$ عدداً أولياً ، فإن m عدد أولي و $a = 2$. أما إذا كــان $a^m + 1$ عــدداً أولياً ، فإن a عدد زوجي و $m = 2^n$ ، ومن هنا كان التعريف الآتي .

تعريف ٥-١-١ :

يقال عن عدد F_n أنه عــدد فيرمــا ، إذا كــان $F_n = 2^{2^n} + 1$ ، $n \in N$. وإذا كان F_n عدداً أولياً ، فيسمى F_n عدد فيرما الأولي .

مثال (١) :

$F_0 = 3$ ، $F_1 = 5$ ، $F_2 = 17$ ، $F_3 = 257$ ، $F_4 = 2^{16} + 1 = 65537$

وهي أعداد أولية ، وعلى الرغم من أن فيرما لم يحسب إلا تلك الأعداد فقد أعتقد أن F_n عدد أولي لكل $n \in N$ ، لكن أويلر أثبت عدم صحة ذلك بإثباتــه بــأن $F_5 = 2^{32} + 1$ يقبــل القــسمة علــى 641 . ونعلــم اليــوم وبإســتخدام برنــامج " Maple " بــأن F_n عــدد مؤلــف لكــل $5 \le n \le 30$ ، وعنــدما $n = 36, 38, 39, 55, 63, 73, 382447$.

ولم يُكتشف لحد الآن أي عدد فيرماتي أولي غيــر F_n ، $0 \le n \le 4$ ولــذلك يعتقد العلماء عدم وجود أعداد فيرما أولية غير تلك الأعداد .

وتبرز أهمية أعداد فيرما الأولية بعد إثبات جاوس سنة ١٧٩٦م بأنه يمكن أن نرسم بالمسطرة والفرجال مضلعاً منتظماً عدد أضلاعه p إذاً وإذا فقــط كــان p عدد فيرما أولي .

ولدراسة خواص أعداد فيرما ، نورد المبرهنات الآتية .

مبرهنة ٥-١-١ :

$\prod_{i=0}^{n-1} F_i = F_n - 2$ لكل $n \in \mathbb{Z}^+$.

البرهان : " بالإستقراء على n "

إذا كان $n = 1$ ، فإن $L.H.S. = F_1 = 3$ ، $R.H.S. = F_1 - 2 = 5 - 2 = 3$ ، وعليه فإن الطرفين متساويان وبالتالي فإن العلاقة صحيحة عندما $n = 1$

والآن لنفرض أن العلاقة صحيحة عندما $n = m$. إذاً

$$\prod_{i=0}^{m-1} F_i = F_m - 2$$

ولكي نثبت صحة العلاقة عندما $n = m + 1$ ، لاحظ أن

$$(\prod_{i=0}^{m-1} F_i) \cdot F_m = (F_m - 2)F_m = (2^{2^m} - 1)(2^{2^m} + 1)$$

$$= (2^{2^{m+1}} - 1) = (2^{2^{m+1}} + 1 - 2) = F_{m+1} - 2$$

إذاً العلاقة صحيحة عندما $n = m + 1$ ، وعليه فإن العلاقة صحيحة لكل $n \in \mathbb{Z}^+$.

□

مبرهنة ٥-١-٢ :

$(F_m , F_n) = 1$ لكل $m, n \geq 0$ و $m \neq n$.

البرهان :

بدون فقدان عمومية البرهان يمكن أن نفرض أن $m < n$. إذاً $n = m + r$ ، وعليه إذا كان $d = (F_m , F_n)$ ، $x = 2^{2^m}$ ، فإن

$$\frac{F_n - 2}{F_m} = \frac{F_{m+r} - 2}{F_m} = \frac{x^{2^r} - 1}{x + 1} = x^{2^r - 1} - x^{2^r - 2} - \cdots - 1$$

وعليه فإن $F_m \backslash (F_n - 2)$. لكن $d \backslash F_m$. إذاً $d \backslash (F_n - 2)$ ، لكن $d \backslash F_n$ إذاً $d \backslash 2$ ، وعليه فإن $d = 1$ أو $d = 2$. لكن أعداد فيرما هي أعداد فردية ، إذاً $d \neq 2$ ، وعليه فإن $d = 1$.

□

ولمعرفة طبيعة القواسم الأولية لأعداد فيرما نورد ما يلي .

تعريف ٥-١-٢ :

إذا كان $n > 1$ عدداً صحيحاً وكان $a \in Z$ و $(a,n) = 1$ ، فيقال عن m أنها رتبة العدد a قياس n ، " Order of a modulo n " ، ونكتب $m = ord_n(a)$ إذا كان m أصغر عدد صحيح موجب بحيث أن $a^m \equiv 1 (\text{mod } n)$.

مثال (٢) :

إذا كان $n = 7$ ، فإن $ord_7(1) = 1$ لأن $1 \equiv 1 (\text{mod } 7)$ ، $ord_7(2) = 3$ لأن $2^3 \equiv 1 (\text{mod } 7)$ ، $ord_7(3) = 6$ لأن $3^6 \equiv 1 (\text{mod } 7)$ ، $ord_7(4) = 3$ لأن $4^3 \equiv 1 (\text{mod } 7)$ ، $ord_7(5) = 6$ لأن $5^6 \equiv 1 (\text{mod } 7)$ ، $ord_7(6) = 2$ لأن $6^2 \equiv 1 (\text{mod } 7)$.

مبرهنة ٥-١-٣ :

إذا كان p عدداً أولياً ، $a \in Z$ ، $(a,p) = 1$ ، $ord_p(a) = n$ ، وكان $a^m \equiv 1 (\text{mod } p)$ ، فإن $n \backslash m$.

البرهان :

نفرض أن $d = (m,n)$. إذاً يوجد $r,s \in Z$ بحيث $d = mr + ns$ حسب مبرهنة (٢-١-٥) . لكن $a^n \equiv a^m \equiv 1 (\text{mod} p)$. إذاً $a^{mr} \equiv a^{nr} \equiv 1 (\text{mod} p)$ وعليه فإن $a^d \equiv a^{mr+ns} \equiv 1 (\text{mod } p)$. لكن n أصغر عدد صحيح موجب بحيث أن $a^n \equiv 1 (\text{mod } p)$. إذاً $n \leq d$. لكن $d \backslash n$ يعني أن $d \leq n$. إذاً $n = d$. لكن $d \backslash m$ ، إذاً $n \backslash m$.

□

نتيجة : إذا كان $p \setminus F_n$ ، فإن $p \equiv 1 (\bmod 2^{n+1})$.

البرهان :

بما أن $p \setminus F_n$. إذاً $2^{2^n} + 1 \equiv 0 (\bmod p)$ ، وعليه فإن $2^{2^n} \equiv -1 (\bmod p)$ ومنها نجد أن $(2^{2^n})^2 = 2^{2^{n+1}} \equiv 1 (\bmod p)$.

والآن أفرض أن $m = ord_p(2)$. إذاً $m \setminus 2^{n+1}$ حسب مبرهنة (٥-١-٣) و $2^m \equiv 1 (\bmod p)$ و $2^{2^{n+1}} \equiv 1 (\bmod p)$ يعني أن $m = 2^{n+1}$. لكن p عدد فردي ، لأن أعداد فيرما أعداد فردية ، إذاً $(p,2) = 1$ ، وعليه فإن $2^{p-1} \equiv 1 (\bmod p)$ حسب مبرهنة فيرما ، وبالتالي فإن $2^{n+1} \setminus (p-1)$ حسب مبرهنة (٥-١-٣) ، ومنها نجد أن $p \equiv 1 \bmod (2^{n+1})$

□

مثال (٣) :

أثبت أن $F_4 = 2^{16} + 1 = 65537$ عدد أولي .

الإثبات :

نفرض أن $p \setminus F_4$. إذاً $p = m \cdot 2^5 + 1$ حسب نتيجة مبرهنة (٥-١-٣) . وعليه فإن $p = 3 \cdot 2^5 + 1 = 97$ أو $p = 8(2^5) + 1 = 257$. لكن $97 \nmid F_4$ و $p = 257 > \sqrt{F_4} \simeq 256 \cdot 0019$. إذاً F_4 عدد أولي حسب نتيجة (٢) مبرهنة (٢-٢-٤) .

□

مثال (٤) :

أثبت أن $F_5 = 2^{2^5} + 1$ عدد مؤلف .

الإثبات :

إذا كان $p \setminus F_5$ ، فإن $p = m \cdot 2^6 + 1$ حسب نتيجة مبرهنة (٥-١-٣) ، وعليه فإن $p = 4(64) + 1 = 257$ أو $p = 10(64) + 1 = 641$. لكن $F_5 = 4294967297$ لا يقبل القسمة على 257 و $p = 641 < \sqrt{F_5} = 65537$ كما أن $F_5 = 641 \times 6700417$. إذاً F_5 عدد مؤلف .

والآن إلى تعريف ودراسة خواص أعداد مرسين .

تعريف ٥-١-٣ :

يقال عن عدد صحيح موجب M_n أنه عدد مرسين (Mersenne number) نسبة للفرنسي مرسين (١٥٨٨-١٦٤٨م) ، إذا كان $M_n = 2^n - 1$ ، $n \geq 2$.
وإذا كان M_n عدداً أولياً فيسمى M_n عدد مرسين الأولي .

لاحظ أنه إذا كان M_n عدداً أولياً ، فإن n عدد أولي حسب مبرهنة (٢-٢-٦)، كما أن هذا النوع من الأعداد معروف لأقليدس (٣٥٠ق.م) ونيقوماخوس (١٠٠ق.م) وثابت بن قرة (٨٢٦-٩٠١م) وغيره من الرياضيين العرب والمسلمين .

مثال (٥) :

$M_2 = 3$ ، $M_3 = 7$ ، $M_5 = 31$ ، $M_7 = 127$ أعداد أولية ، بينما $M_4 = 15$ ، $M_4 = 2047$ ليست أعداد أولية .
ونعرف حالياً وبإستخدام الحاسب الآلي أربعين عدد مرسين أولي M_p عندما

$$p \in \left\{ \begin{array}{l} 2,3,5,7,17,19,31,61,89,107,127,521,607,1279,2203 \\ 2281,3217,4253,4423,9689,9941,11213,19937,21701 \\ 23209,44497,86243,110503,132049,216091,756839 \\ 859433,1257787,1398269,2976221,3021377,6972593 \\ 13466917,25964951 \end{array} \right\}$$

والسؤال الذي يطرح نفسه هو : هل يوجد عدد لا نهائي من أعداد مرسين الأولية ؟

والآن إلى بعض خواص أعداد مرسين وأحدى طرق حسابها .

مبرهنة ٥-١-٤ :

إذا كان p عدداً أولياً فردياً وكان q عدداً أولياً و $q \backslash M_p$ ، فإن

$$q \equiv 1 (\bmod 2p)$$

البرهان :

بما أن $q \setminus M_p$ بالفرض . إذاً $q \setminus 2^p - 1$ ، وعليه فإن $2^p \equiv 1 (\text{mod } q)$.
الآن أفرض أن $\text{ord}_q(2) = m$ نجد أن $m \setminus p$ حسب مبرهنة (٥-١-٣) . لكن p عدد أولي . إذاً $m = p$ وعليه فإن $\text{ord}_q(2) = p$. لكن $2^{q-1} \equiv 1 (\text{mod } q)$ حسب مبرهنة فيرما . إذاً $2 \setminus q - 1$. لكن $(p,2) = 1$. إذاً $2p \setminus q - 1$ ، وعليه فإن $q \equiv 1 \ (\text{mod } 2p)$.

□

مثال (٦) :

أثبت أن كلاً من $M_7 = 127$ ، $M_{13} = 8191$ عدد أولي بينما M_{11} ليس أولياً.

الإثبات :

(أ) بما أن $\sqrt{127} < 12$. إذاً بتطبيق نتيجة (٢) مبرهنة (٢-٢-٤) يكفي أن نبحث عن الأعداد الأولية الأقل من 12 والتي تقسم 127 . لكن $q \setminus 127$ يعطي أن $q = 1 + 14r$ ، $r \geq 1$ حسب مبرهنة (٥-١-٤) . وحيث أن $q > 12$ إذاً لا توجد قواسم للعدد M_7 ، وعليه فإن M_7 عدد أولي .

(ب) بما أن $\sqrt{8191} < 91$. إذاً يكفي أن نبحث عن الأعداد الأولية الأقل من 91 والتي على الشكل $q = 1 + 26r$ ، $r \geq 1$ وهذه الأعداد هي $q = 1 + 26 \times 2 = 53$ أو $q = 1 + 26 \times 3 = 79$. لكن $53 \nmid M_{13}$ و $79 \nmid M_{13}$. إذاً M_{13} عدد أولي .

(ج) بما أن $M_{11} = 2047$ ، $\sqrt{2047} < 46$ ، $q \setminus M_{11}$ يعني أن $q = 1 + 22r$ ، $r \geq 1$ ، وعليه فإن $q = 23 < 46$. لكن $23 \setminus M_{11}$ ، وعليه فإن M_{11} ليس أولياً .

مبرهنة ٥-١-٥ :

إذا كان $r \setminus n$ ، فإن $M_r \setminus M_n$

البرهان : بما أن $n = rs$. إذاً
$M_n = M_{rs} = 2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1)$ ،
لكن $M_r = 2^r - 1$. إذاً $M_r \backslash M_n$.

□

نتيجة : إذا كان M_n عدداً أولياً ، فإن n عدد أولي .

البرهان :

نفرض أن n عدد مؤلف . إذاً $n = rs$ ، $1 < r, s < n$ ، وعليه فإن $M_r \backslash M_n$ حسب مبرهنة (٥-١-٥) . إذاً $M_n = tM_r$. لكن $r > 1$ ، إذاً $M_r > 1$ وحيث أن $r < n$ ، إذاً $M_r < M_n$ ، وبالتالي فإن $t > 1$. إذاً M_n عدد غير أولي وهذا خلاف الفرض . إذاً n عدد أولي .

□

وأخيراً نورد المبرهنة الآتية بدون أثبات لصعوبة البرهان وهذه المبرهنة تبين ما إذا كان M_n عدداً أولياً أم لا .

مبرهنة ٥-١-٦ : " Lucas Criterion 1876 "

إذا كان p عدداً أولياً فردياً وعرفنا المتتابعة $L_1, L_2, \cdots, L_{p-1}$ بالقاعدة $L_1 = 4$ و $L_k = (L_{k-1}^2 - 2) \bmod M_p$ لكل $k \geq 2$ ، فإن M_p عدد أولي إذاً وإذا فقط كان $L_{p-1} = 0$.

مثال (٧) : أثبت أن $M_7 = 127$ عدد أولي .

الإثبات :

$$L_1 = 4 \text{ ، } \quad L_2 = (4^2 - 2) \bmod 127 = 14 \text{ ، }$$

$$L_3 = [(14)^2 - 2] \bmod 127 = 194 \bmod 127 = 67 \text{ ، }$$

$$L_4 = [(67)^2 - 2] \bmod 127 = 4487 \bmod 127 = 42 \text{ ، }$$

$$L_5 = [(42)^2 - 2] \bmod 127 = 1762 \bmod 127 = 111 \text{ ، }$$

$$L_6 = [(111)^2 - 2] \bmod 127 = 12319 \bmod 127 = 0$$

إذاً $M_7 = 127$ عدد أولي حسب مبرهنة (٥-١-٦) .

تمـــــارين

(١) أثبت أن (أ) F_3 عدد أولي ، (ب) F_6 عدد مؤلف .

(٢) أثبت بإستخدام مبرهنة (٥-١-٢) على وجود عدد غير منتهي من الأعداد الأولية.

(٣) برهن بإستخدام مبرهنة (٥-١-١) أن $(F_m, F_n) = 1$ لكل $m \neq n \geq 0$.

(٤) إذا كان $d = (m,n)$ وكان $(M_m, M_n) = M_d$ فأوجد القاسم المشترك الأعظم لكل من :

(أ) M_{11}, M_{23} ، (ب) M_{10}, M_8 ، (ج) M_{61}, M_{122}

(٥) إذا كان $1145 < \sqrt{M_{17}}$ ، فأثبت بإستخدام مبرهنة (٥-١-٤) أن M_{17} عدد أولي.

(٦) أثبت بإستخدام مبرهنة (٥-١-٦) أن $M_{19} = 524281$ عدد أولي .

□

٥-٢ : الأعداد التامة Perfect Numbers

سنركز أهتمامنا في هذا الجزء على دراسة الأعداد التامة والمعرفة من قبل إقليدس .

تعريف ٥-٢-١ :

إذا كانت $\sigma^*(n)$ تمثل مجموع القواسم الفعلية (أجزاء) للعدد الطبيعي n ، فيقال عن n أنه :

(أ) عد زائد (Abundent number) ، إذا كان $\sigma^*(n) > n$.

(ب) عدد ناقص (Deficient number) ، إذا كان $\sigma^*(n) < n$.

لاحظ أن $\sigma(n) = \sigma^*(n) + n$. إذاً

n عدد زائد $\Leftrightarrow$ $\sigma(n) > 2n$

n عدد ناقص $\Leftrightarrow$ $\sigma(n) < 2n$

مثال (١) :

(أ) 12 عـــــــدد زائـــــــد ، لأن $\sigma(n)=\prod_{i=1}^{r}\frac{p_i^{e_i+1}-1}{p_i-1}$ يعنـــــي أن

$\sigma(12)=\sigma(2^2\cdot 3)=\frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}=28>2(12)$.

(ب) 15 عدد ناقص، لأن $\sigma(15)=\sigma(3\cdot 5)=\sigma(3)\cdot\sigma(5)=4(6)<2(15)=30$.

(ج) 945 عدد زائد ، لأن

$$\sigma(945)=\sigma(3^3\cdot 5\cdot 7)=\frac{3^4-1}{3-1}\cdot\frac{5^2-1}{5-1}\cdot\frac{7^2-1}{7-1}=40\cdot 6\cdot 8=1920>2(945)$$

ويقول أبو منصور عبد القادر البغدادي (ت ١٠٣٧م) في مخطوطه " التكملة في الحساب " أن أول عدد زوجي زائد اثنا عشر وكل فرد (عدد فردي) دون تسعمائة وخمسة وأربعين ناقص وأول فرد زائد تسعمائة وخمسة وأربعين " .

مبرهنة ٥-٢-١ : إذا كان $M_p=2^p-1$ عدداً أولياً ، فإن

(أ) $2^p\cdot M_p$ عدد زائد ، (ب) $2^{p-2}\cdot M_p$ عدد ناقص .

البرهان :

(أ) ليكن $n=2^p\cdot M_p$. بما أن $(2^p,M_p)=1$. إذاً

$$\sigma(n)=\sigma(2^p\cdot M_p)=\sigma(2^p)\cdot\sigma(M_p)=(2^{p+1}-1)\cdot\sigma(M_p)$$

لكن M_p عدد أولي . إذاً $\sigma(M_p)=M_p+1$ ، وعليه فإن

$$\sigma(n)=(2^{p+1}-1)\cdot(M_p+1)=(2^{p+1}-1)\cdot 2^p=2^{2p+1}-2^p$$

لكن $2^{p+1}>2^p$. إذاً

$$\sigma(n)=2^{2p+1}-2^p>2^{2p+1}-2^{p+1}$$
$$=2^{p+1}(2^p-1)=2\cdot 2^p(2^p-1)=2n$$

وعليه فإن n عدد زائد .

(ب) ليكن $m = 2^{p-2} \cdot M_p$. بما أن $(2^{p-2}, M_p) = 1$ إذاً

$$\sigma(m) = \sigma(2^{p-2}) \cdot \sigma(M_p) = (2^{p-1} - 1)(M_p + 1) = (2^{p-1} - 1) \cdot 2^p$$
$$= 2^{2p-1} - 2^p < 2^{2p-1} - 2^{p-1} = 2^{p-1}(2^p - 1)$$
$$= 2 \cdot 2^{p-2}(2^p - 1) = 2m$$

وبالتالي فإن m عدد ناقص .

□

<u>مبرهنة ٥-٢-٢ :</u>

(أ) يوجد عدد لا نهائي من الأعداد الناقصة .

(ب) يوجد عدد لا نهائي من الأعداد الزائدة .

<u>البرهان :</u>

(أ) ليكن $n = p^m$ ، حيث p عدد أولي فردي و $m \geq 1$. إذاً

$$\sigma(n) = (1 + p + p^2 + \cdots + p^{m-1}) + p^m < p^m + p^m = 2p^m = 2n$$

وعليه فإن n عدد ناقص . لكن $S = \{p^m | m \geq 1$ و P عدد أولي فردي$\}$ مجموعة غير منتهية . إذاً يوجد عدد لا نهائي من الأعداد الناقصة .

(ب) ليكن $n = 945m$ ، $(945, m) = 1, m > 1$. إذاً

$$\sigma(n) = \sigma(945) \cdot \sigma(m)$$

لكن 945 عدد زائد . إذاً $\sigma(945) > 2(945)$. كما أن $\sigma(m) > m$ لكل $m > 1$. إذاً $\sigma(n) > 2(945m) = 2n$ ، وعليه فإن n عدد زائد . لكن $S = \{945m | m > 1 ، (945, m) = 1\}$ مجموعة غير منتهية . إذاً يوجد عدد غير منتهي من الأعداد الزائدة .

□

والآن إلى تعريف الأعداد الطبيعية التامة ودراسة خواصها .

تعريف ٥-٢-٢ :

يقال عن عدد طبيعي n أنه عدد تام (Perfect number) إذا كان $\sigma^*(n) = n$.

إذاً n عدد تام $\Leftrightarrow \sigma(n) = 2n$.

مثال (٢) : كل من $6, 28, 496, 8128$ عدد تام ، لأن

$$\sigma(6) = \sigma(2 \cdot 3) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} = 3 \cdot 4 = 12 = 2(6) \text{ ،}$$

$$\sigma(28) = \sigma(2^2 \cdot 7) = \frac{2^3 - 1}{2 - 1} \cdot \frac{7^2 - 1}{7 - 1} = 7 \cdot 8 = 56 = 2(28)$$

$$\begin{aligned}\sigma(496) &= \sigma(2^4 \cdot 31) = \sigma(2^4) \cdot \sigma(31) = (2^5 - 1) \cdot 31 = 31 \cdot 32 \\ &= 2(2^4 \cdot 31) = 2(496)\end{aligned}$$

$$\begin{aligned}\sigma(8128) &= \sigma(2^6 \cdot 127) = \sigma(2^6) \cdot \sigma(127) = (2^7 - 1) \cdot 128 = 127 \cdot 128 \\ &= 2(2^6 \cdot 127) = 2(8128)\end{aligned}$$

ولقد وردت تلك الأعداد عند ميناخوس اليوناني حوالي (١٠٠م) .

والآن إلى قاعدة تحديد الأعداد التامة الزوجية والتى تعود إلى إقليدس .

مبرهنة ٥-٢-٣ : " **إقليدس** "

إذا كان $M_p = 2^p - 1$ عدداً أولياً ، فإن $n = 2^{p-1} \cdot M_p$ عدد تام .

البرهان :

بما أن $(2^{p-1}, M_p) = 1$. إذاً

$$\begin{aligned}\sigma(n) &= \sigma(2^{p-1} \cdot M_p) = \sigma(2^{p-1}) \cdot \sigma(M_p) = (2^p - 1)\,(M_p + 1) \\ &= (2^p - 1) \cdot 2^p = 2 \cdot 2^{p-1} \cdot M_p = 2n\end{aligned}$$

وعليه فإن n عدد تام .

□

واستناداً لتلك القاعدة ، نجد أن

العدد التام الأول هو 6 ، لأن $M_2 = 3$ عدد أولي و $6 = 2 \cdot M_2$.

العـــدد التـــام الثـــاني يـــساوي 28 ، لأن $M_3 = 2^3 - 1 = 7$ عـــدد أولـــي و $2^2 \cdot M_3 = 2^2 \cdot 7 = 28$.

العـــدد التـــام الثالـــث يـــساوي 496 ، لأن $M_5 = 2^5 - 1 = 31$ عـــدد أولـــي $2^4 M_5 = 2^4 \cdot 31 = 496$.

العدد التام الرابـــع يـــساوي 8128 ، لأن $M_7 = 2^7 - 1 = 127$ عـــدد أولـــي و $2^6 \cdot M_7 = 2^6 \cdot 127 = 8128$.

العدد التام الخامس يساوي 33550336 ،لأن $M_{13} = 2^{13} - 1 = 8191$ عدد أولي و $2^{12} \cdot M_{13} = (4096) \cdot 8191 = 33550336$.

العدد التام الـــسادس يـــساوي 8589869056 ، لأن $M_{17} = 2^{17} - 1 = 131071$ عدد أولي و $8589869056 = 2^{16} \cdot M_{17}$.

هذا ويُعرف إلى الآن سبعة وعشرين عدداً تماماً تنتج عندما يكون

$$P \in \begin{Bmatrix} 2,3,5,7,13,17,19,31,61,89,107,257,521,607 \\ 1279,2203,2281,3217,4253,4423,9689 \\ 9941,11213,19937,21701,23209,44497 \end{Bmatrix}$$

لاحظ أن عكس مبرهنة (٥-٢-٣) صحيح أيضاً، وهذا ما توضحه المبرهنة الآتية .

<u>مبرهنة ٥-٢-٤ :</u> " ابن الهيثم - أويلر "

إذا كان n عدداً زوجياً تاماً ، فإن $n = 2^{p-1}(2^p - 1)$ و $(2^p - 1)$ عدد أولي .

<u>البرهان :</u>

بما أن n عدد زوجي . إذاً $n = 2r$ ، $r \in Z^+$ ، وعليه بعد تجميع جميع قوى العدد 2 في r يُمكننا أن نعبر عن n بالشكل الآتي $n = 2^{p-1} \cdot m$ ، $p \geq 2$ ، m عدد فردي . إذاً $(2^{p-1}, m) = 1$ ، وعليه فإن

$$\sigma(n) = \sigma(2^{p-1} \cdot m) = \sigma(2^{p-1}) \cdot \sigma(m) = (2^p - 1)\sigma(m) \qquad \dots (1)$$

لكن n عدد تام . إذاً

$$\sigma(n) = \sigma(2^{p-1} \cdot m) = 2(2^{p-1} \cdot m) = 2^p \cdot m \qquad \dots (2)$$

ومن (1) ، (2) ينتج أن

$$(2^p-1)\sigma(m)=2^p\cdot m \qquad \dots (3)$$

ومنها نجد أن $(2^p-1)\backslash 2^p\cdot m$. لكن $(2^p,2^p-1)=1$ ، إذاً $(2^p-1)\backslash m$ حسب مبرهنة (٢-١-٩ب) ، وعليه فإن

$$m=(2^p-1)t=2^p\cdot t-t \text{ ، } t\in Z^+ \qquad \dots (4)$$

ومن (3) ، (4) ينتج أن $\sigma(m)=2^p\cdot t$. لكن كلاً من m،t قاسم للعدد m و $t<m$ يعني أن $2^p\cdot t=\sigma(m)\geq m+t$.

ومن (4) نجد أن $m+t=2^p\cdot t$ ، إذاً

$$2^p\cdot t=\sigma(m)\geq m+t=2^p\cdot t=\sigma(m)$$

وعليه فإن $\sigma(m)=m+t$ وهذا يعني أن $\tau(m)=2$ ، وعليه فإن m عدد أولي.

إذاً $t=1$ ، وعليه فإن $m=2^p-1$ عدد أولي و $n=2^{p-1}(2^p-1)$.

□

هذا ونود أن نشير إلى أن عبدالقادر البغدادي قد ذكر في مخطوطه " التكملة في الحساب " ما يلي :

" **وقد غلط من قال في كل عقد من العقود عدد واحد تام وأصاب من قال كل عدد تام لابد أن يكون في أوله ستة أو ثمانية** " ثم يذكر بعد ذلك قاعدة تشكيل الأعداد التامة السابقة ، ويقترح القاعدة الآتية والتي تنص على الآتي :

" **إذا كان أجزاء زوج الزوج أوليه ، فإن مجموع آحادها من الواحد إليها يكون تاماً** " .

أي أنه إذا كان $M_n=2^n-1$ عدداً أولياً ، فإن $[1+2+3+\cdots+(2^n-1)]$ عدد تام . لأن $1,2,3,\dots,2^n-1$ متوالية عددية حدها الأول واحد وحدها الأخير (2^n-1) ، وعليه فإن مجموعها هو

$$\frac{2^n-1}{2}[1+2^n-1]=2^{n-1}(2^n-1)$$

وحسب قاعدة البغدادي يكون العدد التام الأول(6) والثاني (28) والثالث(496) وهكذا

مبرهنة ٥-٢-٥ : " البغدادي "

كل عدد زوجي تام لابد أن يكون آحاده ستة أو ثمانية .

أي أن إذا كان n عدداً زوجياً تاماً، فإن $n \equiv 6 \pmod{10}$ أو $n \equiv 8 \pmod{10}$

البرهان :

بما أن n عدد زوجي تام . إذاً $n = 2^{p-1}(2^p - 1)$ و $(2^p - 1)$ عدد أولي حسب مبرهنة (٥-١-٤) . لكن $(2^p - 1)$ عدد أولي يعني أن p عدد أولي حسب مبرهنة (٢-٢-٦) .

فإذا كان $p = 2$ ، فإن $n = 6$ و $6 \equiv 6 \pmod{10}$ ، وعليه فإن المبرهنة صحيحة . أما إذا كان $p > 2$ ، فإن p عدد أولي فردي ، وعليه فإن $p = 4m + 1$ أو $p = 4m + 3$ حسب مبرهنة (٢-١-٣ب) .

فإذا كان $p = 4m + 1$ ، فإن

$$n = 2^{4m}(2^{4m+1} - 1) = 2^{8m+1} - 2^{4m} = 2 \cdot 2^{8m} - 2^{4m} = 2 \cdot (16)^{2m} - (16)^m$$

لكن $(16)^r \equiv 6 \pmod{10}$ لكل $r \in Z^+$. إذاً

$$n \equiv 2 \cdot 6 - 6 \equiv 6 \pmod{10}$$

أما إذا كان $p = 4m + 3$ ، فإن

$$n = 2^{4m+2}(2^{4m+3} - 1) = 2^{8m+5} - 2^{4m+2} = 2(16)^{2m+1} - 4(16)^m$$
$$\equiv 2 \cdot 6 - 4 \cdot 6 \equiv -12 \equiv 8 \pmod{10}$$

□

لاحظ أن المبرهنات السابقة تصف الأعداد الزوجية التامة إما الأعداد الفردية التامة ، فلم يستطع أحد حتى الآن أن يجيب على سؤال الرياضي والفلكي والفيزيائي أبو جعفر الخازن أحد علماء القرن العاشر للميلاد وهو :

هل يوجد عدد تام فردي ؟

وعلى الرغم من ذلك فقد حدد أويلر خواص الأعداد الفردية التامة في المبرهنة الآتية .

مبرهنة ٥-١-٦ : " أويلر "

إذا كان n عدداً فردياً تاماً ، فإن $n = p_1^{e_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r}$ ، حيث p_i أعداد أولية فردية مختلفة و $p_1 \equiv e_1 \equiv 1 \pmod 4$.

البرهان :

نفرض أن $n = \prod_{i=1}^{r} p_i^{e_i}$. بما أن n عدد تام . إذاً $2n = \sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{e_i})$ لكن n عدد فردي ، إذاً $n \equiv 1 \pmod 4$ أو $n = 3 \pmod 4$ حسب مبرهنة (٢-١-٣ب) ، وفي كلتا الحالتين نجد أن $2n \equiv 2 \pmod 4$ ، وعليه فإن $\sigma(n) = 2n$ يقبل القسمة على 2 ولا يقبل القسمة على 4 . إذاً $2 \setminus \sigma(p_i^{e_i})$ لبعض قيم i حسب مبرهنة (٢-٢-٣ب) ، وعليه فإن $\sigma(p_i^{e_i})$ عدد زوجي لبعض قيم i ، وبدون فقدان عمومية البرهان يمكن أن نفرض أن $\sigma(p_1^{e_1})$ عدد زوجي لا يقبل القسمة على 4 بينما $\sigma(p_i^{e_i})$ عدد فردي لكل $i \neq 1$.

والآن $p_i \equiv 1 \pmod 4$ أو $p_i \equiv 3 \pmod 4$ حسب مبرهنة (٢-١-٣ب)

فإذا كان $p_i \equiv 3 \equiv -1 \pmod 4$ ، فإن

$$\sigma(p_i^{e_i}) = 1 + p_i + p_{i^2} + \cdots + p_i^{e_i}$$
$$\equiv 1 + (-1) + (-1)^2 + \cdots + (-1)^{e_i} \pmod 4$$
$$\equiv \begin{cases} 0 \pmod 4 & \text{إذا كان } e_i \text{ عدد فردي} \\ 1 \pmod 4 & \text{إذا كان } e_i \text{ عدد زوجي} \end{cases}$$

لكن $\sigma(p_1^{e_1}) \equiv 2 \pmod 4$ يعني أن $p_1 \not\equiv 3 \pmod 4$ ، وعليه فإن $p_1 \equiv 1 \pmod 4$. وحيث أن $\sigma(p_i^{e_i}) \equiv 0 \pmod 4$ يعني أن $4 \setminus \sigma(p_i^{e_i})$ وهذا غير ممكن كما أثبتنا أعلاه . إذاً إذا كان $p_i \equiv 3 \pmod 4$ لكل $i = 2, \ldots, r$ ، فإن e_i عدد زوجي . أما إذا كان $p_i \equiv 1 \pmod 4$ ، فإن

$$\sigma(p_i^{e_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{e_i} \equiv 1 + 1 + 1^2 + \cdots + 1^{e_i} \pmod 4$$
$$\equiv e_i + 1 \pmod 4$$

لكن $\sigma(p_1^{e_1}) \equiv 2 \pmod 4$ يعني أن $e_1 \equiv 1 \pmod 4$. أما لكل $i = 2,...,r$ فـــإن $\sigma(p_i^{e_i}) \equiv 1 \pmod 4$ أو $\sigma(p_i^{e_i}) \equiv 3 \pmod 4$ ، وذلـــك يعنـــي أن $e_i \equiv 0 \pmod 4$ أو $e_i \equiv 2 \pmod 4$ وفي كلتا الحالتين نجـد أن e_i عـدد زوجي . إذاً $e_i = 2\alpha_i$ لكل $i = 2,...,r$ ، وعليه فـإن $n = p_1^{e_1}(\prod_{i=2}^{r} p_i^{2\alpha_i})$ و $p_1 \equiv e_1 \equiv 1 \pmod 4$.

□

نتيجة :

إذا كان n عدداً فردياً تاماً ، فإن $n = p^r m^2 \equiv 1 \pmod 4$ و p عدد أولي و $p \nmid m$ ، $p \equiv r \equiv 1 \pmod 4$.

البرهان :

بمـــا أن $n = p_1^{e_1} \prod_{i=2}^{r} p_i^{2\alpha_i}$ حـــسب مبرهنـــة (٥-١-٦) . إذاً $n = p_1^{e_1}(\prod_{i=2}^{r} p_i^{\alpha_i})^2 = p^r \cdot m^2$ ، حيـث $m = \prod_{i=2}^{r} p_i^{\alpha_i}$ ، $p_1^{e_1} = p^r$. لكـن $p \equiv 1 \pmod 4$ يعني أن $p^r \equiv 1 \pmod 4$. أما m عدد فردي فإن ذلك يعني أن $m \equiv 1 \pmod 4$ أو $m \equiv 3 \pmod 4$ حسب مبرهنة (٢-١-٣ب) ، وعليه فإن $m^2 \equiv 1 \pmod 4$ ، وبالتالي فإن $n = p^r \cdot m^2 \equiv 1 \cdot 1 \equiv 1 \pmod 4$.

□

تمـــارين

(١) برهن على وجود عدد غير منتهي من الأعداد الفردية الناقصة .

(٢) برهن على وجود عدد غير منتهي من الأعداد الفردية الزائدة وعدد غيـر منتهي من الأعداد الزوجية الزائدة .

(٣) أثبت أن $2^{10}(2^{11}-1)$ عدد غير تام .

(٤) أثبت أن كلاً من $2^{606}(2^{607}-1)$ ، $2^{1278}(2^{1279}-1)$ عدد تام .

(٥) إذا كان $n=p^m$ ، $m\geq 1$ ، p عدد أولي ، فأثبت أن n عدد غير تام .

(٦) إذا كان $n=a^2$ ، $a\in Z^+$ ، فأثبت أن n عدد غير تام .

(٧) إذا كان n عدداً تاماً ، فأثبت أن nr عدد تام لكل $r\geq 1$.

(٨) إذا كان n عدداً تاماً ، فأثبت أن $\sum_{d\backslash n}\frac{1}{d}=2$ وحقق ذلك عندما $n=6$ و $n=22$.

(٩) إذا كان n عدداً زوجياً تاماً ، فأثبت أن $\phi(n)=2^{p-1}(2^{p-1}-1)$.

(١٠) إذا كان p,q عددين أوليين فرديين مختلفين وكان $n=pq$ ، فأثبت أن n عدد غير تام . "لاحظ أن $\sigma(n)=pq+p+q+1$ و $pq>p+q+1$ "

(١١) إذا كان (2^p-1) عدداً أولياً ، فأثبت أن
$(2^{p-1}+2^p+2^{p+1}+\cdots+2^{2p-2})$ عدد تام .

(١٢) إذا كان $n>6$ عدداً زوجياً تاماً ، فأثبت أن $n\equiv 4(\text{mod } 6)$.
"لاحظ أن $n=2^{p-1}(2^p-1)>6$ يعني أن $p>3$ ، وعليه فإن $p=4m+1$ أو $p=4m+3$ " .

(١٣) إذا كان n عدداً فردياً تاماً ، فأثبت أن $n=pa^2$ حيث p عدد أولي .

(١٤) إذا كان $n=pa^2$ عدد فردياً تاماً ، فأثبت أن $n\equiv p(\text{mod } 8)$.

٥-٣ : الأعداد المتحابة والأعداد المتعادلة

نتناول في هذا الجزء الأعداد المتحابة المعرّفة من قبل فيثاغورس والأعداد المتعادلة المعرفة من قبل عبد القادر البغدادي في القرن العاشر للميلاد.

تعريف ٥-٣-١ :

يقال عن عددين طبيعيين m,n أنهما متحابان (Amicable) . إذا كان

$\sigma^*(n)=m$ و $\sigma^*(m)=n$

إذاً m,n متحابان $\Leftrightarrow \sigma(m)=\sigma(n)=m+n$

مثال (١) :

220 ، 284 متحابان ، لأن $284+220=504$ و

$$\sigma(220)=\sigma(2^2\cdot5\cdot11)=\frac{2^3-1}{2-1}\cdot\frac{5^2-1}{5-1}\cdot\frac{11^2-1}{11-1}=7\cdot6\cdot12=504$$

$$\sigma(284)=\sigma(2^2\cdot71)=\sigma(2^2)\cdot\sigma(71)=\frac{2^3-1}{2-1}\cdot(72)=7\cdot72=504$$

ملاحظة :

إذا كان $\sigma(m)=\sigma(n)$ فإن ذلك لا يعني أن n،m متحابان كما يوضح ذلك المثال الآتي .

ليكن $m=6$ ، $n=11$. إذاً $\sigma(m)=\sigma(n)=12$. لكن 6،11 غير متحابين لأن $\sigma^*(m)=6\neq11=n$ ، وعليه فإن الشرط $\sigma(m)=\sigma(n)=m+n$ ضروري .

والآن إلى قاعدة تحديد بعض الأعداد المتحابة والتي تنسب إلى ثابت بن قرة الحراني (٨٢٦ م _ ٩٠١م) .

مبرهنة ٥-٣-١ : "قاعدة بن قرة "

إذا كان $a=3\cdot2^n-1$ ، $b=3\cdot2^{n-1}-1$ ، $c=9\cdot2^{2n-1}-1$ أعداداً أولية فإن 2^nab ، 2^nc عددان متحابان .

البرهان

بما أن $2^n, a, b$ أعداد أولية نسبياً مثنى مثنى و σ داله ضربية. إذاً

$\sigma(2^n ab) = \sigma(2^n)\cdot\sigma(a)\cdot\sigma(b)$. لكـــن $\sigma(2^n) = 2^{n+1} - 1$ و a،b عددان أوليـــان . إذاً $\sigma(a) = a + 1 = 3\cdot 2^n$ ، $\sigma(b) = b + 1 = 3\cdot 2^{n-1}$ ، وعليه فإن

$$\sigma(2^n ab) = (2^{n+1} - 1)\cdot 9\cdot 2^{2n-1} = 9\cdot 2^{2n-1}(2^{n+1} - 1) \qquad \ldots (1)$$

وحيث أن $(2^n, c) = 1$. إذاً

$$\sigma(2^n c) = \sigma(2^n)\cdot\sigma(c) = (2^{n+1} - 1)\cdot 9\cdot 2^{2n-1}$$
$$= 9\cdot 2^{2n-1}\cdot(2^{n+1} - 1) \qquad \cdots (2)$$

ومن (1) ، (2) نجد أن

$$\sigma(2^n ab) = \sigma(2^n c) \qquad \ldots (3)$$. لكن

$$2^n ab + 2^n c = 2^n(ab + c) = 2^n(9\cdot 2^{2n-1} - 9\cdot 2^{n-1} + 1 + 9\cdot 2^{2n-1} - 1)$$
$$= 2^n(9\cdot 2^{2n} - 9\cdot 2^{n-1}) = 9\cdot 2^{2n-1}(2^{n+1}) \qquad \cdots (4)$$

ومن (3) ، (4) نجدان $\sigma(2^n ab) = \sigma(2^n c) = 2^n ab + 2^n c$ ، وعليـــه فـــإن $2^n ab$ ، $2^n c$ عددان متحابان.

□

هذا وقد درست الأعداد التامة والأعداد المتحابة في النصف الثاني من القـــرن العاشر للميلاد من قبل أبو صقر القبيصي في بحثه " في جمع أنواع من الأعـــداد " ذاكراً قاعدة تشكيل الأعداد التامة ومبرهنة بن قرة عن الأعداد المتحابـــة بالـــشكل الآتي :

إذا كـــــــــــــان $a = (2^{n+1} - 1) + 2^n$ ، $b = (2^{n+1} - 1) - 2^{n-1}$ ، $c = 2^{n+1}(2^{n+1} + 2^{n-2}) - 1$ أعداداً أوليـــة ، فـــإن $2^n ab$ ، $2^n c$ عـــددان متحابان .

كما أفرد الكرخي (ت ٤٢١هـ) في كتابة (البديع في الحساب : تحقيق عادل أنبوبا) فصلاً عن الأعداد المتحابة قدم فيه برهاناً عاماً لقاعدة بن قرة مستنتجاً ما يلي :

إذا كان (m,n) زوج من الأعداد المتحابة فمن الضروري أن يكون أحدهما ناقصاً والآخر زائداً ، كما أن $m-\sigma^*(m)=\sigma^*(n)-n$. ثم يثبت أنه إذا كان a,b,c ثلاثة أعداد أولية فردية بحيث أن

$$2>s=\sum_{i=0}^{n}2^i \quad ، \quad c-s=(1+a+b)s-ab$$

فإن $2^n ab$ ، $2^n c$ عددان متحابان و $2^n c$ عدد ناقص بينما $2^n ab$ عددان زائد .

أما عبد القادر البغدادي فقد تعرض في كتابه " التكملة في الحساب " للأعداد المتحابة ومبرهنة بن قرة . وأما أبن سينا (٩٨٠ــ١٠٣٧م) فقد ذكر في كتابه (الشفاء : الطبيعيات) ما يلي :

إذا كانت $(2^{n+1}-1)$ ، $a=3\cdot 2^n-1$ ، $b=3\cdot 2^{n-1}-1$ أعداداً أولية، فإن $2^n ab$ ، $2^n(a+b+ab)=2^n(9\cdot 2^{2n-1}-1)$ عددان متحابان ، فإذا أضفنا الشرط $(9\cdot 2^{2n-1}-1)$ عدد أولي نجد مبرهنة بن قرة مع الشرط الزائد $(2^{n+1}-1)$ هو أولي .

أما الزنجاني (ت ١٢٥٧م) فقد أعاد في بحثه "عمدة الحساب" نتائج البغدادي وأعطى مبرهنة بن قرة حول الأعداد المتحابة .

أما كمال الدين الفارس (ت١٣٢٠م) فقد أعاد في مخطوطه "تذكرة الأحباب في تمام التحاب" أثبات مبرهنة بن قرة ، كما وردت مبرهنة بن قرة عند زين الدين التنوخي وابن يعيش الأموي ، كما وردت عند الكاشي (ولد في كاشان سنة ٦٥٤هـ) في كتابه "مفتاح الحساب" وعند شرف الدين اليزدي ومحمد باقر اليزدي.

هذا وبتطبيق مبرهنة بن قرة عندما $n = 2$ نجد أن $a = 11$ ، $b = 5$ ، $c = 71$ وهي أعداد أولية ، وعليه فإن $2^2ab = 220$ ، $2^2c = 284$ عددان متحابان . وإذا كان $n = 4$ ، فإن $a = 47$ ، $b = 23$ ، $c = 1151$ أعداد أولية ، وعليه فإن $2^4ab = 2^4 \cdot 47 \cdot 23 = 17296$ ، $2^4 \cdot c = 2^4 \cdot 1151 = 18416$ عددان متحابان . وقد حسب هذين العددين كل من كمال الدين الفارسي في كتابه (تذكرة الأحباب في بيان التحاب) – وعلي بن عبد القادر بن هيدور التادلي (ت١٤١٣م) قبل الفرنسي فيرما (١٦٠١ـ ١٦٦٥م) الذي ينسبان إليه ، ولقد بين الفارسي أن $\sigma^*(18416) = 17296$ ، $\sigma^*(17296) = 18416$ كالآتي :

$$\sigma^*(17296) = \sigma^*(2^4 \cdot 23 \cdot 47) = \sigma^*(2^4)\sigma^*(23 \cdot 47) + 2^4\sigma^*(23 \cdot 47)$$
$$= 15(71 + 1081) + 16(71) = 18416$$

إما

$$\sigma^*(18416) = \sigma^*(2^4 \cdot 1151) = \sigma^*(2^4)(1151 + 1) + 2^4$$
$$= 15 \cdot 1152 + 16 = 17296$$

أما الزوج (9363584,9437056) والذي ينسب إلى الفرنسي ديكارت (١٥٩٦- ١٦٥٠م) فقد حُسبَ من قبل محمد باقر اليزدي (ت١٦٣٠م) بتطبيق مبرهنة بن قرة عندما $n = 7$ فوجد أن $a = 383$ ، $b = 191$ ، $c = 73727$ أعداد أولية ، وعليه فإن $2^7c = 9437056$ ، $2^7ab = 9363584$ عددان متحابان .

وأخيراً نود أن نشير إلى أن أويلر قد عمم مبرهنة بن قرة واكتشف فيما بين (١٧٤٧ ـ ١٧٥٠م) تسعة وخمسين زوجاً من الأعداد المتحابة منها.

(10856،10744) ، (6368،6232) ، (5020،5564) ، (2924،2620)

وأكتشف الزوج (1210,1184) والذي لا يمكن الحصول عليه بتطبيق قاعدة بن قرة عام ١٨٦٧م من قبل الإيطالي نيقولو باغنيني ، وأكتشف لحد الآن 900 زوج من الأعداد المتحابة .

والآن إلى تعريف الأعداد المتعادلة المعرفة منذ القرن العاشر للميلاد من قبل عبد القادر البغدادي في كتابة "التكملة في الحساب" .

تعريف ٥-٣-٢ :

يقال عن عددين طبيعيين m,n أنهما متعادلان (Numbers of equal weight) إذا كان $\sigma^*(m)=\sigma^*(n)$.

إذاً n،m متعادلان $\Leftrightarrow \quad \sigma^*(m)+n=\sigma(n)+m$

ويقال عن $a_1,\dots,a_n$ أنها أعداد متعادلة ، إذا كان

$$\sigma^*(a_1)=\sigma^*(a_2)=\cdots=\sigma^*(a_n)$$

مثال (٢) :

(أ) العددان 39 ، 5 متعادلان ، لأن

$$\sigma^*(39)=1+3+13=17 \quad ، \quad \sigma^*(55)=1+5+11=17$$

(ب) الأعداد $a=111$ ، $b=319$ ، $c=391$ متعادلة ، لأن

$$\sigma^*(391)=1+23+17=41 \; ، \; \sigma^*(319)=1+11+29=41$$

$$\sigma^*(a)=1+3+37=41$$

ولقد ذكر البغدادي أنه : إذا كان معنا عدد مفروض ، وأردنا أن نعلم الأعداد التي مجموع أجزاء كل واحد منها مثل هذا العدد المفروض ، أنقصنا من العدد المفروض واحداً ثم جزئنا الباقي بعددين أوليين وقسمنا أيضاً بعددين آخرين أوليين وهكذا ، ثم نضرب القسمين في التقسيم الأول أحدهما في الآخر ، ونضرب القسمين في التقسيم الثاني أحدهما في الآخر وكذلك نفعل بقسمي التقسيم الثالث والرابع ....، وما يعدّ مما أصبح من هذه الضروب ، وكل منها أجزاءه مثل ذلك العدد المفروض أي أن :

إذا كان a عدداً طبيعياً معلوماً ، وكان المطلوب إيجاد جميع الأعداد المتعادلة المرتبطة بالعدد a ، يُعبر عن a بالشكل الآتي :

$a=1+p_i+q_i$ حيث p_i , q_i أعداد أولية مختلفة لكل $i=1,2,\dots$ فنجد أن $\{p_i \, q_i\}$ أعداد مختلفة مجموع أجزائها متساوي .

ويعطي البغدادي المثال الآتي :

مثال (٣) :

إذا كان $a = 57$ ، فإن $a - 1 = 56$ و $56 = 3 + 53$ ، $56 = 13 + 43$ و 3,13,43,53 أعداد أولية مختلفة ، وعليه فإن $m = 3 \cdot 53 = 159$ ، $n = 13 \cdot 43 = 559$ عددان متعادلان ، لأن $\sigma^*(m) = \sigma^*(n) = 57$.

لاحظ أن الزنجاني في "عمدة الحساب" أعطى نفس التعريف السابق ونفس المثال مثبتاً أن 159 ، 559 ، 703 أعداد متعادلة ، لأن

$$\sigma^*(703) = 1 + 19 - 37 = 57$$

مثال (٤) :

أوجد جميع الأعداد المتعادلة المرتبطة بالعدد 49 .

الحل :

لاحظ أن المطلوب هو إيجاد جميع الأعداد التي مجموع القواسم الفعلية لكل منها يساوي 49 ، ولإيجاد تلك الأعداد نعبر عن العدد 49 بالشكل $49 = 1 + p_i + q_i$ حيث p_i, q_i أعداد أولية مختلفة ، وعليه فإن $p_i + q_i = 48$ وبالتالي فإن

$$(p_i, q_i) = (5,43)\ ,\ (7,41)\ ,\ (11,37)\ ,\ (17,31)\ ,\ (19,29)$$

وعليه فإن الأعداد هي

$$a_1 = p_i q_i = 5 \cdot 43 = 215,\ a_2 = 7 \cdot 41 = 287, a_3 = 11 \cdot 37 = 407$$
$$a_4 = 17 \cdot 31 = 527\ ,\ a_5 = 19 \cdot 29 = 551$$

هذا ونجد فيما بعد دراسة للأعداد المتعادلة في الكثير من الأبحاث الحسابية ، ويحدد محمد باقر اليزدي (ت ١٦٣٧م) العلاقة الآتية : **إذا عبرنا عن عدد زوجي كمجموع عددين أوليين وضربناهما في بعضهما وسُمي العدد الناتج m ثم عبرنا عن ذلك العدد الزوجي بطريقة أخرى وضربناهما في بعضهما ، وسميّ العدد الناتج n ، لوجدنا أن العددين m,n متعادلان .**

مثال (٥) :

(أ) $16 = 3 + 13 \Rightarrow n = 3 \cdot 13 = 39$, $16 = 5 + 11 \Rightarrow m = 5 \cdot 11 = 55$ و

m,n متعادلان

(ب) إذا كان $a = 36$ ، فإن

$$36 = 5 + 31 \Rightarrow a_1 = 5 \cdot 31 = 155, 36 = 7 + 29 \Rightarrow a_2 = 7 \cdot 29 = 203$$

$$36 = 13 + 23 \Rightarrow a_3 = 13 \cdot 23 = 299, 36 = 17 + 19 \Rightarrow a_4 = 17 \cdot 19 = 323$$

و $a_1, a_2, a_3\ a_4$ أعداد متعادلة ، لأن

$$\sigma^*(a_1) = \sigma^*(a_2) = \sigma^*(a_3) = \sigma^*(4) = 37$$

تمـــــارين

(١) برهن أن كل زوج من الأعداد الآتية يمثل عددين متحابين :

(أ) 1184،1210 ، (ب) 5564،5020 ، (ج) 6232،6368

(د) 14595،12285

(٢) إذا كان m,n عددين متحابين وكان $m > n$ ، فأثبت أن m عدد ناقص بينما n عدد زائد .

(٣) إذا كان m,n عددين متحابين ، فأثبـــت أن $(\sum_{d\backslash m}\frac{1}{d})^{-1} + (\sum_{d\backslash n}\frac{1}{d})^{-1} = 1$ ، وحقق تلك العلاقة عندما $m = 220$ ، $n = 284$.

(٤) أوجد جميع الأعداد المتعادلة المرتبطة بالعدد n عندما $n = 61$ ، $n = 65$ ، $n = 90$.

****

الفصل السادس

البواقي التربيعية وقانون التعاكس الثنائي
Quadratic Residues and Quadratic Reciprocity Law

يضم هذا الفصل ثلاثة بنود ندرس فيها الجذور البدائية ووجودها ، البواقي التربيعية وخواصها ورمزي لجندر وجاكوبي وقانون التعاكس وبعض تطبيقاتها .

٦-١ : الجذور البدائية Prmitive Roots

سنركز أهتمامنا في هذا الجزء على تعريف وتحديد الجذور البدائية والتي وردت في أبحاث أويلر عام ١٧٧٣م ولجندر (١٧٥٢-١٨٣٣) عام ١٧٨٥م وجاوس عام ١٨٠١م ، وسنبرهن على وجود مثل تلك الجذور لأي عدد أولي ، ثم ندرس الشروط التي يجب توفيرها لكي يكون لعدد طبيعي أكبر من الواحد جذراً بدائياً .

تعريف ٦-١-١ :

ليكن a,n عددين طبيعيين . يقال عن a أنه جذر بدائي أو إبتدائي (Primitive Root) قياس n (جذر بدائي للعدد n) إذا كان $a^{\phi(n)} \equiv 1 (\mathrm{mod}\ n)$ بينما $a^m \not\equiv 1 (\mathrm{mod}\ n)$ لكل $m < \phi(n)$.

إذاً a جذر بدائي قياس $n \Leftrightarrow \mathrm{ord}_n(a) = \phi(n)$.

مثال (١) :

(أ) 2,3 جذران بدائيان قياس 5 ، لأن $\phi(5) = 4$ و $2^4 \equiv 1 (\mathrm{mod}\ 5)$ ، $3^4 \equiv 1 (\mathrm{mod}\ 5)$.

(ب) 5,3 جذر بدائيان قياس 7 ، لأن $\phi(7) = 6$ و $3^6 \equiv 1 (\mathrm{mod}\ 7)$ ، $5^6 \equiv 1 (\mathrm{mod}\ 7)$.

مثال (٢) :

إذا كان $n = 9$ ، فإن 2,5 جذران بدائيان قياس 9 ، لأن $\phi(9) = 6$ و $2^6 \equiv 1 (\mathrm{mod}\ 9)$ ، $5^6 \equiv 1 (\mathrm{mod}\ 9)$.

مثال (٣) :

2 ليست جذراً بدائياً قياس 257 ، لأن $16 = \text{ord}_{257}(2) \neq \phi(257) = 2^8$.

مثال (٤) :

لا يوجد جذر بدائي قياس 8 ، لأن $\phi(8) = 4$ و $\text{ord}_8(a) \neq 4$ لكل $a \in Z_8^* = \{1,2,3,4,5,6,7\}$.

وبصورة عامة يمكن أن نبرهن ما يلي .

مبرهنة ٦-١-١ :

إذا كان $m \geq 3$ ، فليس للعدد 2^m جذر إبتدائي .

البرهان :

ليكن $(a,2^m) = 1$. إذاً a عدد فردي . سنثبت بالإستقراء على m أن

$$a^{2^{m-2}} \equiv 1 (\text{mod } 2^m) \text{ لكل } m \geq 3 \quad \ldots (1)$$

فإذا كان $m = 3$ ، فإن (1) تعني أن $a^2 \equiv 1(\text{mod } 8)$ وهذه علاقة صحيحة ، لأن $1^2 = 3^2 = 5^2 = 7^2 \equiv 1 \ (\text{mod } 8)$.

والآن لنفرض أن العلاقة (1) صحيحة عندما $m = k$. إذاً

$$a^{2^{k-2}} \equiv 1(\text{mod } 2^k)$$

ولإثبات صحة العلاقة عندما $m = k+1$ ، لاحظ أن

$$a^{2^{k-2}} \equiv 1(\text{mod } 2^k) \Leftrightarrow a^{2^{k-2}} = 1 + b \cdot 2^k \ , b \in Z$$

وعليه فإن

$$a^{2^{k-1}} = (a^{2^{k-2}})^2 = (1 + b \cdot 2^k)^2 = 1 + 2b \cdot 2^k + b^2 \cdot 2^k$$
$$= 1 + 2^{k+1}(b + b^2 \cdot 2^{k-1}) \equiv 1(\text{mod } 2^{k+1})$$

وبالتالي فإن العلاقة (1) صحيحة عندما $m = k+1$. إذاً العلاقة (1) صحيحة لكل $m \geq 3$. لكن $\phi(2^m) = 2^{m-1}$ و $a^{2^{m-2}} \equiv 1 \ (\text{mod } 2^m)$.

يعني أن $a^{\frac{\phi(2^m)}{2}} \equiv 1 \pmod{2^m}$ ، وعليه فـإن $ord_{2^m}(a) \neq \phi(2^m)$ إذاً لا يوجد جذر بدائي قياس 2^m .

□

الآن إلى المبرهنة الآتية التي تساعدنا في تحديد عدد الجذور البدائية لعدد طبيعي n .

مبرهنة ٦-١-٢ :

ليكن $(a,n)=1$ و $R=\{a_1,a_2,\cdots,a_{\phi(n)}\}$ نظام بواقي مختزل قياس n . إذا كان a جذراً بدائياً للعدد n ، فإن كل عنصر من عناصر $S=\{a,a^2,\cdots,a^{\phi(n)}\}$ يوافق عنصر وحيد من عناصر R .

البرهان :

بما أن $(a,n)=1$. إذاً $(a^m,n)=1$ لكل $m=1,\cdots,\phi(n)$. لكن $a^i \not\equiv a^j \pmod{n}$ لكل $i \neq j$ و R نظام بواقي مختزل قياس n . إذاً $a_r \not\equiv a_s \pmod{n}$ لكل $r \neq s$ ، وعليه فإن لكل a^m يوجد عنصر وحيد $a_i \in R$ بحيث أن $a^m \equiv a_i \pmod{n}$.

□

نتيجة :

إذا كان للعدد n جذراً بدائياً فإن عدد الجذور البدائية للعدد n يساوي $\phi(\phi(n))$.

البرهان :

نفرض أن a جذر بدائي للعدد n ، إذاً الجذور البدائية الأخرى للعدد n تنتمي إلى المجموعة $S=\{a,a^2,\cdots,a^{\phi(n)}\}$ حسب مبرهنة (٦-١-٢) . لكن

$$\left|\{a^m \mid 1\le m\le \phi(n),\ ord_n(a^m)=\phi(n)\}\right|$$
$$=\left|\{m: 1\le m\le \phi(n), (m,\phi(n)=1\}\right|=\phi(\phi(n))$$

وهذا يعني أن عدد الجذور البدائية للعدد n يساوي $\phi(\phi(n))$.

□

مثال (٥) :

حقق مبرهنة (٦-١-٢) ونتيجتها عندما $n=9$.

الحل :

بما أن $\phi(9)=6$ ، 2 جذر بدائي قياس 9 . إذاً $S=\{2,2^2,2^3,2^4,2^5,2^6\}$ ، $R=\{1,2,4,5,7,8\}$ و

$$2\equiv 2(\text{mod } 9)\ ,\ 2^2=4(\text{mod } 9)\ ,\ 2^3\equiv 8(\text{mod } 9)\ ,\ 2^4\equiv 7(\text{mod } 9)$$

$$2^5\equiv 5(\text{mod } 9)\ \ ,\ 2^6\equiv 1(\text{mod } 9)$$

لكن $\phi(\phi(9))=\phi(6)=2$ ، وعليه يوجد جذر بدائي آخر قياس 9 ولإيجاده ، لاحظ أن $(1,6)=(5,6)=1$. إذاً $r=5$ جذر بدائي قياس 9 .

مثال (٦) :

إذا كان 2 جذراً بدائياً للعدد 27 ، فأوجد الجذر البدائي الآخر .

الحل :

بما أن $\phi(27)=3^3(1-\frac{1}{3})=18$ ، $\phi(\phi(27))=\phi(18)=6$. إذاً توجد خمسة جذور بدائية أخرى للعدد 27 ، ولإيجادها لاحظ أن

$$(1,18)=(5,18)=(7,18)=(11,18)=(13,18)=(17,18)=1$$

وعليه فإن كلاً 2,5,7,11,13,17 جذر بدائي للعدد 27 .

ولكي نبرهن على وجود جذور بدائية ، ونحدد طبيعة الأعداد التي تملك مثل تلك الجذور نورد المبرهنات الآتية .

مبرهنة ٦-١-٣ : " لاجرانج "

إذا كان p عدداً أولياً ، وكانت $f(x)=\sum_{i=0}^{n}a_ix^i$ ، $a_i\in Z$ ، $a_n\not\equiv 0(\text{mod } p)$ كثيرة حدود من الدرجة n ، فإن للعلاقة $f(x)\equiv 0(\text{mod } p)$ ، على الأكثر n من الحلول غير المتطابقة قياس p .

البرهان : "بالإستقراء على n "

فإذا كان $n=1$ ، فإن $f(x)=a_0+a_1x$ و $(a_1,p)=1$ ، وعليه فإن للعلاقة الخطية $a_1x\equiv -a_0 \pmod p$ حل وحيد قياس p حسب مبرهنة (٣-٤-١) . إذاً المبرهنة صحيحة عندما $n=1$.

والآن لنفرض أن المبرهنة صحيحة عندما $n=k$ ولإثبات صحتها عندما $n=k+1$ ، لاحظ أنه أما $f(x)\equiv 0 \pmod p$ لا تملك حلاً أو أنها تملك على الأقل حل واحد وليكن $x=a$. إذاً

$$f(x)\equiv (x-a)g(x) \pmod p \quad ، \quad \deg(g(x))=k$$

وحيث أن $f(b)\equiv 0 \pmod p \Leftrightarrow g(b)\equiv 0 \pmod p$ لكل $a\not\equiv b \pmod p$ إذاً أي حل للعلاقة $g(x)\equiv 0 \pmod p$ هو حل للعلاقة $f(x)\equiv 0 \pmod p$ لكن للعلاقة $g(x)\equiv 0 \pmod p$ ، على الأكثر k من الحلول غير المتطابقة قياس p حسب فرضية الإستقراء الرياضي . إذاً للعلاقة $f(x)\equiv 0 \pmod p$ على الأكثر $(k+1)$ من الحلول غير المتطابقة قياس p ، وعليه فإن المبرهنة صحيحة عندما $n=k+1$. إذاً المبرهنة صحيحة لكل $n\geq 1$.

□

نتيجة :

إذا كان p عدداً أولياً و $n\setminus(p-1)$ ، فإن للعلاقة $x^n-1\equiv 0 \pmod p$ ، n من الحلول .

البرهان :

بما أن $n\setminus(p-1)$. إذاً يوجد $m\in Z$ بحيث أن $p-1=mn$ ، وعليه فإن

$$x^{p-1}-1=(x^n)^m-1=(x^n-1)[x^{n(m-1)}+x^{n(m-2)}+\cdots+x^n+1]$$
$$=(x^n-1)g(x)$$

حيث $g(x)=x^{n(m-1)}+\cdots+x^n+1$ ، $\deg(g(x))=n(m-1)=p-1-n$

لكن $g(x)\equiv 0 \pmod p$ تملك على الأكثر $(p-1-n)$ من الحلول غير

المتطابقة قياس p حسب مبرهنة (٦-١-٣) ، ومن مبرهنة فيرما نجد أن للعلاقة $x^{p-1}-1\equiv 0 \pmod p$ ، $(p-1)$ من الحلول غير المتطابقة قياس p وهي $1,2,3,\dots,p-1$ ، كما أن $a^{p-1}-1\equiv 0 \pmod p$ و $g(a)\not\equiv 0 \pmod p$ يعني أن $a^n-1\equiv 0 \pmod p$ ، وعليه يجب أن يكون للعلاقة $x^n-1\equiv 0 \pmod p$ ، على الأقل n من الحلول . لكن للعلاقة $x^n-1\equiv 0 \pmod p$ ، على الأكثر n من الحلول حسب مبرهنة (٦-١-٣) . إذاً يوجد للعلاقة $x^n-1\equiv 0 \pmod p$ ، n من الحلول .

□

والآن إلى المبرهنة الآتية والتي أثبتها أويلر سنة ١٧٧٣م وحسب جميع الجذور البدائية لكل الأعداد الأولية $p\le 37$.

مبرهنة ٦-١-٤ :

يوجد جذر بدائي لأي عدد أولي p .

البرهان :

إذا كان $p=2$ ، فإن $ord_2(1)=\phi(2)=1$ ، وعليه فإن الواحد جذر بدائي قياس 2 . وإذا كان $p>2$ فإن $(p-1)>1$ ، وعليه فإن $p-1=\prod_{i=1}^{r}p_i^{e_i}$ حسب المبرهنة الأساسية في الحساب . ومن نتيجة مبرهنة (٦-١-٣) نجد أن للعلاقة $x^{p_i^{e_i}}-1\equiv 0 \pmod p$ ، بالضبط $p_i^{e_i}$ من الجذور (من الحلول غير المتطابقة)، ولكثيرة الحدود $x^{p_i^{e_i-1}}-1\equiv 0 \pmod p$ بالضبط $p_i^{e_i-1}$ من الحلول غير المتطابقة ، وعليه يوجد $p_i^{e_i}-p_i^{e_i-1}=p_i^{e_i-1}(p_i-1)$ عنصراً رتبة كل منها تساوي $p_i^{e_i}$. إذاً لكل $i=1,\dots,r$ يمكن نختار عنصر a_i, $ord_p(a_i)=p_i^{e_i}$ ، وعليه إذا كان $a=a_1a_2\dots a_r$ ، فإن $ord_p(a)=\prod_{i=1}^{r}p_i^{e_i}=p-1=\phi(p)$ ، وعليه فإن a جذر بدائي قياس p .

مثال (٧) :

لتكن $p=13$. إذاً $p-1=12=2^2\cdot 3$ ، ولكثيرة الحدود $x^4-1=0 \bmod 13$ أربعة جذور هي $1,5,8,12$ أما لكثيرة الحدود $x^2-1=0 \pmod{13}$ جذران هما $1,12$. إذاً يمكن أن يكون $a_1=5$ لكن لكثيرة الحدود $x^3-1=0 \pmod{13}$ ثلاثة جذور هي $1,3,9$ ، وعليه يمكن أن نضع $a_2=3$ ويكون $a=a_1a_2=5\cdot 3=15\equiv 2 \pmod{13}$ جذراً بدائياً قياس 13 . لأن $ord_{13}(2)=\phi(13)=12$. لاحظ أن بقية الجذور البدائية هي

$$8\cdot 3=11 \pmod{13}\ ,\ 8\cdot 9=7 \pmod{13}\ ,\ 5\cdot 9=6 \pmod{13}$$

لأن $ord_{13}(11)=12\ ,\ ord_{13}(7)=12\ ,\ ord_{13}(6)=12$.

مبرهنة ٦-١-٥ :

إذا كان p عدداً أولياً فردياً وكان r جذراً بدائياً قياس p ، فإن r أو $r+p$ جذر بدائي قياس p^m لكل $m\ge 1$.

البرهان :

بما أن r جذر بدائي قياس p . إذاً $ord_p(r)=p-1$. فإذا كان $r^{p-1}\equiv 1 \pmod{p^2}$ ، فإن

$$(r+p)^{p-1}=r^{p-1}+\binom{p-1}{1}r^{p-2}\cdot p+\cdots+p^{p-1}$$
$$\equiv 1+(p-1)pr^{p-2} \pmod{p^2}$$
$$\equiv (1-p\cdot r^{p-2}) \pmod{p^2} \not\equiv 1 \pmod{p^2}$$

إذاً إذا وضعنا r بدلاً من $r+p$ ، يمكننا أن نفرض أن $r^{p-1}\not\equiv 1 \pmod{p^2}$.
وحيث أن $r^{p-1}\equiv 1 \pmod{p}$. إذاً $r^{p-1}=1+ap$ ، $a\in\mathbb{Z}$ ، $p\nmid a$. لكن $(1+ap)^{p^{m-1}}\equiv (1+ap)^m \pmod{p^{m+1}}$ لكل $m\ge 1$. إذاً
$ord_{p^m}(r^{p-1})=ord_{p^m}(1+ap)=p^{m-1}$ لكل $m\ge 1$ ، وعليه فإن

أصغر عدد صحيح موجب k يجعل $(r^{p-1})^k \equiv 1 (\text{mod } p^m)$ هو $k = p^{m-1}$
وبالتالي فإن أصغر عدد صحيح موجب t بحيث أن $r^t \equiv 1 \ (\text{mod } p^m)$ هو
$t = (p-1)k = (p-1)p^{m-1}$. لكن $\phi(p^m) = (p-1)p^{m-1}$. إذاً
$r^{\phi(p^m)} \equiv 1 \ (\text{mod } p^m)$ ، وعليه فإن r جذر بدائي قياس p^m لكل $m \ge 1$.

□

نتيجة :

إذا كان p عدداً أولياً فردياً ، فإن للعدد $2p^m$ جذور بدائية لكل $m \ge 1$.

البرهان :

بما أن p عدد أولي فردي . إذاً يوجد جذر بدائي قياس p^m لكل $m \ge 1$ حسب مبرهنة (٦-١-٥) ، وعليه نفرض أن r جذر بدائي قياس p^m .

إذا كان r عدداً زوجياً ، فإن $r + p^m$ عدد فردي . ومن الواضح أن $r + p^m$ جذر بدائي قياس p^m ، وعليه يمكن أن نفرض أن r عدد فردي .
إذاً $(r, 2p^m) = 1$ ، وعليه فإن $r^{\phi(2p^m)} \equiv 1 (\text{mod } 2p^m)$ حسب مبرهنة أويلر .
فإذا كان $\text{ord}_{2p^m}(r) = n$ ، فإن $n \setminus \phi(2p^m)$ حسب مبرهنة (٥-١-٣) .
وحيث أن $\phi(2p^m) = \phi(2)\phi(p^m) = \phi(p^m)$ و
$r^n \equiv 1 (\text{mod } 2p^m) \Rightarrow r^n \equiv 1 \ (\text{mod } 2p^m)$ ،
$\text{ord}_{p^m} = \phi(p^m) = \phi(2p^m)$. إذاً $\phi(2p^m) \setminus n$ حسب مبرهنة (٥-١-٣) .
وعليه فإن $n = \phi(2p^m)$ وبالتالي فإن r جذر بدائي قياس $2p^m$.

□

مبرهنة ٦-١-٦ :

إذا كان $a > 2$ ، $b > 2$ أعداداً طبيعيةً ، $(a, b) = 1$ ، فإن ab لا يملك جذراً بدائياً .

البرهان :

ليكن $c \in Z$ و $(ab,c)=1$. إذاً $(a,c)=(b,c)=1$ ، وعليه إذا كان $m=[\phi(a),\phi(b)]$ و $d=(\phi(a),\phi(b))$ ، فإن كلاً من $\phi(a),\phi(b)$ عدد زوجي حسب مبرهنة (٤-٣-٤) ، كما أن $d \geq 2$ ، وبالتالي فإن

$$m=\frac{\phi(a)\ \phi(b)}{d} \leq \frac{\phi(ab)}{2} \qquad \ldots(1)$$

لكن $c^{\phi(a)} \equiv 1 \pmod a$ حسب مبرهنة أويلر . إذاً

$$c^m=(c^{\phi(a)})^{\frac{\phi(b)}{d}} \equiv 1 \pmod a$$

وبالمثل نجد أن $c^m \equiv 1 \pmod b$. لكن $(a,b)=1$. إذاً $c^m \equiv 1 \pmod{ab}$

وعليه فإن $\phi(ab) > \frac{\phi(ab)}{2} \geq m \geq ord_{ab}(c)$ حسب (١) . وبالتالي فإن c ليست جذراً بدائياً قياس ab . إذاً ab لا يملك جذر بدائي .

□

نتيجة :

إذا كان p عدداً أولياً فردياً ، فإن $n=2^m p^k$ ، $m \geq 2$ لا يملك جذراً بدائياً .

البرهان :

بما أن $2^m>2$ ، $p^k>2$ ، $(2^m,p^k)=1$. إذاً $n=2^m p^k$ لا يملك جذراً بدائياً حسب مبرهنة (٦-١-٦) .

□

والآن إلى المبرهنة التي تحدد طبيعة الأعداد التي تملك جذور بدائية .

مبرهنة ٦-١-٧ : " جاوس ١٨٠١م "

إذا كان $n>1$ فإن n يملك جذراً بدائياً ، إذاً وإذا فقط كان $n=2,4,p^m,2p^m$ ، حيث p عدد أولي فردي و $m \geq 1$.

البرهان :

من المبرهنتين (٦-١-١) و (٦-١-٦) ، نجد أن الأعداد التي تملك جذوراً بدائية هي $2,4,p^m,2p^m$ حيث p عدد أولي فردي و $m \geq 1$.

ولإثبات العكس لاحظ أن الواحد جذر بدائي للعدد 2 أما 3 فهو جذر بدائي للعدد 4 ، لأن $ord_4(3) = \phi(4) = 2$. وإذا كان $n = p^m$ أو $n = 2p^m$ ، حيث p عدد أولي فردي و $m \geq 1$ فإن مبرهنة (٦-١-٤) و مبرهنة (٦-١-٥) ونتيجتها تضمن وجود جذر بدائي للعدد n .

□

وكتطبيق على ما سبق نورد المثال الآتي .

مثال (٨) :

إذا كان 3 جذراً بدائياً للعدد 43 ، فأوجد جميع الأعداد الموجبة a الأقل من 43 ، بحيث $ord_{43}(a) = 6$.

الحل :

بما أن $\phi(6) = 2$. إذاً يوجد عددان رتبة كل منهما تساوي 6 قياس 43 . ولمعرفة هذين العددين ، لاحظ أن 3 جذر بدائي للعدد 43 . ورتبة 3^m ، $1 \leq m \leq 42$ هي

$$ord_{43}(3^4) = \frac{42}{(m,42)} = 6 \Leftrightarrow (m,42) = 7$$

إذاً $m = 7,35$. لكن $3^4 \equiv -5 \pmod{43}$ ، $3^3 \equiv -16 \pmod{43}$ يعني أن $3^7 \equiv 80 \equiv 37 \pmod{43}$ ، وعليه فإن أحد العددين هو 37 . ولتحديد العدد الثاني . لاحظ أن $3^{35} \equiv (3^7)^5 \equiv (-6)^5 \bmod (43)$. لكن $3^7 \equiv -6 \pmod{43} \Rightarrow$ $(-6)^2 \equiv -7 \pmod{43} \Rightarrow (-6)^4 \equiv 49 \equiv 6 \pmod{43}$. إذاً $(-6)^5 \equiv -36 \equiv 7 \pmod{43}$ ، وعليه فإن $3^{35} \equiv 7 \pmod{43}$. وبالتالي فإن العدد الثاني هو 7 . إذاً $a = 7,37$.

وأخيراً إلى تخميني جاوس وارتين حول الجذور البدائية واللذّين لم تثبت صحتهما أو خطأهما إلى الآن .

وينص تخمين جاوس (Gauss Conjecture) والذي نشر عام ١٨٠١م على الآتي " **يوجد عدد لا نهائي من الأعداد الأولية يكون العدد 10 جذراً بدائياً لكل منها** "

إما تخمين الألماني ارتين (١٨٩٣-١٩٦٢) والذي نشر عام ١٩٢٧م فهو تعميم لتخمين جاوس ، وينص على الآتي

" **إذا كان** $a \in Z$ ، $a \neq \mp 1$ **و a ليس مربعاً كاملاً ، فيوجد عدد غير منتهي من الأعداد الأولية يكون a جذراً بدائياً لكل منها** " .

تمارين

(١) أثبت أن 2 جذر بدائي للعدد 19 ، ثم أوجد بقيمة الجذور البدائية للعدد 19 .

(٢) أثبت أن 15 لا يملك جذراً بدائياً .

(٣) أوجد الجذور البدائية للعدد 17 ، علماً بأن 3 واحد منها .

(٤) أوجد جذرين بدائيين للعدد 10 .

(٥) إذا كان $F_n = 2^{2^n} + 1$ عدداً أولياً ، فأثبت أن 2 ليست جذراً بدائياً للعدد F_n . " لاحظ أن $F_n \setminus (2^{2^{n+1}} - 1)$ " .

(٦) أوجد الجذور البدائية لكل من 26 ، 25 ، 81 .

(٧) أثبت أن 3 جذر بدائي لكل من 7^m ، $2 \cdot 7^m$ لكل $m \geq 1$.

(٨) إذا كان n يقبل القسمة على عددين أوليين مختلفين ، فأثبت أن n لا تملك جذراً أبتدائياً . " طبق مبرهنة (٦-١-٦) " .

(٩) إذا كان p عدداً أولياً فردياً وكان r جذراً بدائياً إلى p^n ، فأثبت أن r جذر بدائي للعدد p .

(١٠) (أ) إذا كان $ord_n(a) = r$ وكان $s > 0$ ، فأثبت أن $ord_n(a^s) = \frac{r}{(r,s)}$
ثم أستنتج من ذلك أن $ord_n(a^s) = r \Leftrightarrow (r,s) = 1$.

(ب) إذا كان 3 جذراً بدائياً لكل من 43،31 فأوجد جميع الأعداد الموجبة a الأقل من 31 بحيث أن $ord_{31}(a) = 6$ ، ثم أوجد جميع الأعداد الموجبة b الأقل من 43 بحيث أن $ord_{31}(a) = 21$.

(١١) إذا كان p عدداً أولياً فردياً وكان r جذر بدائي إلى p^m ، فأثبت أن r جذر بدائي إلى $2p^m$ ، إذاً وإذا فقط كان r عدداً صحيحاً فردياً ، ثم أستنتج من ذلك أن $3, 3^3, 3^5, 3^9$ جذور بدائية إلى $578 = 2(17)^2$.

(١٢) إذا كان r جذراً بدائياً للعدد الأولي p وكان $(r + tp)^{p-1} \not\equiv 1 \pmod{p^2}$ ، فأثبت أن $(r + tp)$ جذر بدائية إلى p^m لكل $m \geq 1$.

(١٣) إذا كان $a, n \in Z$ وكان $a^{n-1} \equiv 1 \pmod{n}$ و $a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$ لكل قاسم أولي q للعدد $(p-1)$ ، فأثبت أن n عدد أولي و a جذر بدائي له .

(١٤) إذا كان r جذراً بدائياً للعدد n ، فأثبت أن r^m جذر بدائي للعدد n . إذاً وإذا فقط كان $(m, \phi(n)) = 1$.

٦-٢ : البواقي التربيعية Quadratic Residues

أن وجود أو عدم وجود حل للتطابق $x^2 \equiv a \pmod{n}$ ، $(a,n) = 1$ يقود إلى ما يسمى البواقي التربيعية وغير التربيعية ، والتي ظهرت في أبحاث أويلر سنة ١٧٧٣م وأبحاث الفرنسي لجندر ١٧٨٥م ، وأبحاث جاوس ١٨٠١م وهذا ما نرغب بدراسته في هذا الجزء .

تعريف ٦-٢-١ :

إذا كان $n \in Z^+$ ، فيقال عن $a \in Z$ أنه باقي تربيعي (Quadaratic Residue) قياس n ، إذا كان $(a,n)=1$ ويوجد $x \in Z$ بحيث أن $x^2 \equiv a \pmod{n}$.

أما إذا كان $(a,n)=1$ ولا يوجد $x \in Z$ بحيث أن $x^2 \equiv a \pmod{n}$ فيقال عن a أنه باقي غير تربيعي (Quadratic Nonresidue) قياس n .

إذا كان a باقياً تربيعياً قياس n فيعبر عن ذلك بالشكل aRn . أما إذا كان a باقياً غير تربيعي قياس n ، فيعبر عن ذلك بالشكل aN_n . لاحظ أن

$$a \equiv b \pmod{n} \Rightarrow (aRn \Leftrightarrow bRn)$$

مثال (١) :

إذا كان $n=5$ ، فإن $2^2 \equiv 3^3 \equiv 4 \pmod{5}$, $1^2 \equiv 4^2 \equiv 1 \pmod{5}$ و $(1,5)=(4,5)=1$. إذاً aR_5 لكل $a \in \{1,4\}$ و aN_5 لكل $a \in \{2,3\}$.

لاحظ أن

$$\left|\{a \in Z_5^* : aR_5\}\right| = \left|\{a \in Z_5^* : aN_5\}\right| = \frac{5-1}{2} = 2$$

مثال (٢) :

إذا كان $n=7$ ، فإن $1^2 \equiv 6^2 \equiv 1 \pmod{7}$ ، $3^2 \equiv 4^2 \equiv 2 \pmod{7}$ ، $2^2 \equiv 5^2 \equiv 4 \pmod{7}$ ، $(1,7)=(2,7)=(4,7)=1$. إذاً aR_7 لكل $a \in \{1,2,4\}$. وحيث أن $(3,7)=(5,7)=(6,7)=1$ و $x^2 \not\equiv 3 \pmod{7}$ ، $x^2 \not\equiv 5 \pmod{7}$ ، $x^2 \not\equiv 6 \pmod{7}$ لكل $x \in Z_7^*$ إذاً aN_7 لكل $a \in \{3,5,6\}$. لاحظ أن

$$\left|\{a \in Z_7^* : aR_7\}\right| = \left|\{a \in Z_7^* : aN_7\}\right| = \frac{7-1}{2} = 3$$

مثال (٣) :

إذا كان $n = 9$ ، فإن $(1,9) = (2,9) = (4,9) = (5,9) = (7,9) = (8,9) = 1$

و $1^2 \equiv 8^2 \equiv 1(\text{mod } 9)$ ، $2^2 \equiv 7^2 \equiv 4(\text{mod } 9)$ ،

$4^2 \equiv 5^2 \equiv 7(\text{mod } 9)$. إذاً aR_9 لكل $a \in \{1,4,7\}$. أما aN_9 فلكل $a \in \{3,5,8\}$. لاحظ أن

$$\left|\{a \in Z_9^* : aR_9\}\right| = \left|\{a \in Z_9^* : aN_9\}\right| = \frac{3(3-1)}{2} = 3$$

مثال (٤) :

إذا كان $n = 11$ ، فإن $(a,n) = 1$ لكل $a \in \{1,2,3,4,5,6,7,8,9,10\}$ ،

كما أن $3^2 \equiv 8^2 \equiv 9(\text{mod } 11)$, $2^2 \equiv 9^2 \equiv 4(\text{mod } 11)$,

$1^2 \equiv 10^2 \equiv 1(\text{mod } 11)$, $5^2 \equiv 6^2 \equiv 3(\text{mod } 11)$, $4^2 \equiv 7^2 \equiv 5(\text{mod } 11)$,

إذاً aR_{11} لكل $a \in \{1,3,4,9\}$ بينما aN_{11} لكل $a \in \{2,6,7,8,10\}$ وأن

$$\left|\{a \in Z_{11}^* : aR_{11}\}\right| = \left|\{a \in Z_{11}^* : aN_{11}\}\right| = \frac{(11-1)}{2} = 6$$

مثال (٥) :

إذا كان $n = 15 = 3 \cdot 5$ ، فإن $\phi(15) = \{1,2,4,7,8,11,13,14\}$ و

$2^2 \equiv 7^2 \equiv 8^2 \equiv (13)^2 \equiv 4(\text{mod } 15)$ و $1^2 \equiv 4^2 \equiv (11)^2 \equiv (14)^2 \equiv 1(\text{mod } 15)$

إذاً aR_{15} لكل $a \in \{1,4\}$ بينما aN_{15} لكل $a \in \{2,7,8,11,13,14\}$. لاحظ أن

$$\left|a \in Z_{15}^* : aR_{15}\right| = \frac{\phi(15)}{2^2} = 2$$

وبصورة عامة إذا كان $n = \prod_{i=1}^{r} p_i^{e_i}$ عدداً صحيحاً فردياً فإن

$$\left|\{a \in Z_n^* : aR_n\}\right| = \frac{\phi(n)}{2^r}$$

مثال (٦) :

إذا كـــان $n = 27 = 3^3$ ، فـــإن $\phi(27) = 18$ ، $(a,27) = 1$ لكـــل

$a \in \{1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26\}$ و

$2^2 \equiv (25)^2 \equiv 4(\text{mod } 27)\,,\, 4^2 \equiv 23^2 \equiv 16(\text{mod } 27)$ ،

$5^2 \equiv (22)^2 \equiv 25(\text{mod } 27)$ ، $1^2 \equiv (26)^2 \equiv 1(\text{mod } 27)$

$10^2 \equiv (17)^2 \equiv 19(\text{mod } 27)$ ، $7^2 \equiv (20)^2 \equiv 22(\text{mod } 27)$ ،

$(13)^2 \equiv (14)^2 \equiv 7(\text{mod } 27)$ ، $8^2 \equiv (19)^2 \equiv 10(\text{mod } 27)$ ،

$(11)^2 \equiv (16)^2 \equiv 13(\text{mod } 27)$

وعليه فإن aR_{27} لكل $a \in \{1,4,7,10,13,16,19,22,25\}$ و aN_{27} لكـــل $a \in \{2,5,8,11,14,17,20,23,26\}$. كما أن

$$\left|\{a \in Z_{27}^* : aR_{27}\}\right| = \left|\{a \in Z_{27}^* : aN_{27}\}\right| = \frac{3^2(3-1)}{2} = 9$$

وبصورة عامة إذا كان $n = p^m$ عدد فردياً فإن

$$\left|\{a \in Z_{p^m}^* : aR_{p^m}\}\right| = \left|\{a \in Z_{p^m}^* : aN_{p^m}\}\right| = \frac{(p-1)p^{m-1}}{2}$$

وهذا ما توضحه المبرهنة الآتية

مبرهنة ٦-٢-١ :

إذا كان p عدداً أولياً فردياً وكان $a \in Z$ و (a,p^m) ، $m \geq 1$ ، فإن

(أ) $aR\,p^m$ إذاً وإذا فقط كان $a^{\frac{p^{m-1}\cdot(p-1)}{2}} \equiv 1(\text{mod } p^m)$.

(ب) aNp^m إذاً وإذا كان $a^{\frac{p^{m-1}\cdot(p-1)}{2}} \equiv -1(\text{mod } p^m)$.

(ج) $aR\,p^m$ إذاً وإذا فقط كان aR_p .

البرهان

(أ) نفرض أن aRp^m . إذاً يوجد حل x_1 للتطابق $x^2 \equiv a \pmod{p^m}$ ، وعليه فإن $x_1^2 \equiv a \pmod{p^m}$. لكن $(a,p^m)=1$. إذاً $(x,p^m)=1$ ، وعليه فإن

$$a^{p^{m-1}\cdot(\frac{p-1}{2})} = (x_1^2)^{p^{m-1}\cdot\frac{p-1}{2}} = x_1^{p^{m-1}(p-1)} = x_1^{\phi(p^m)} \equiv 1 \pmod{p^m}$$

حسب مبرهنة أويلر (٣-٥-١) .

ولإثبات العكس نفرض أن $a^{p^{m-1}\cdot\frac{p-1}{2}} \equiv 1 \pmod{p^m}$ وأن r جذر بدائي قياس p^m . إذاً $a = r^k$ لبعض قيم k حيث $1 \le k \le (p^m - 1)$ ، وعليه فإن

$$r^{p^{m-1}(\frac{p-1}{2})k} \equiv a^{p^{m-1}\cdot(\frac{p-1}{2})} \equiv 1 \pmod{p^m}$$

لكن $\mathrm{ord}_{p^m}(r) = \phi(p^m) = p^{m-1}(p-1)$. إذاً $kp^{m-1}(\frac{p-1}{2})$ يقبل القسمة على $p^{m-1}(p-1)$ حسب مبرهنة (٥-١-٣) ، وعليه فإن $k = 2t$ ، $t \in Z$ وبالتالي فإن $(r^t)^2 = r^k \equiv a \pmod{p^m}$ ، وعليه فإن r^t حل للتطابق $x^2 \equiv a \pmod{p^m}$ ، وبالتالي فإن aRp^m .

(ب) نفرض أن $aNp^m, (a,p^m)=1$. إذاً $a^{\phi(p^m)} \equiv 1 \pmod{p^m}$ حسب مبرهنة أويلر (٣-٥-١) . لكن

$$a^{\phi(p^m)} - 1 = a^{p^{m-1}(p-1)} - 1 = (a^{\frac{p-1}{2}\cdot p^{m-1}} - 1)(a^{\frac{p-1}{2}\cdot p^{m-1}} + 1) \equiv 0 \pmod{p^m}$$

و $a^{\frac{p-1}{2}\cdot p^{m-1}} - 1 \not\equiv 0 \pmod{p^m}$ ، لأنه إذا كان $a^{\frac{p-1}{2}\cdot p^{m-1}} - 1 \equiv 0 \pmod{p^m}$ ، فإن aRp^m حسب(أ) وهذا خلاف الفرض.

إذاً $a^{\frac{p-1}{2}\cdot p^{m-1}} \equiv -1 \pmod{p^m}$.

ولإثبات العكس أفرض أن aRp^m تجد أن $a^{\frac{p-1}{2}\cdot p^{m-1}} \equiv 1 \pmod{p^m}$ ، وعليه إذا كان $a^{\frac{p-1}{2}\cdot p^{m-1}} \equiv -1 \pmod{p^m}$ ، فإن aNp^m .

(ج) نفـــرض أن $aR\,p^m$. إذاً $a^{\frac{p-1}{2}.p^{m-1}} \equiv 1 (\mathrm{mod}\ p^m)$ ، وعليـــه فـــإن $a^{\frac{p-1}{2}.p^{m-1}} \equiv 1 (\mathrm{mod}\ p)$ وبالتالي فإن $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p)$ حسب مبرهنة فيرما . وبوضع $m = 1$ في (أ) نجد أن $aR\,p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p)$.

ولإثبات العكس نفرض أن $aR\,p$ إذاً $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p)$. وحيث أن

$$\forall m \geq 1 , a \equiv b\ (\mathrm{mod}\ p^m) \Rightarrow a^p \equiv b^p\ (\mathrm{mod}\ p^{m+1})$$

إذاً $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p) \Rightarrow a^{\frac{p-1}{2}.p^{m-1}} \equiv 1 (\mathrm{mod}\ p^m)$ ، وعليـــه فـــإن $aR\,p^m$ حسب (أ) .

□

<u>نتيجة :</u> (Euler's Criterion)

إذا كان p عدداً أولياً فردياً ، $(a,p) = 1$ فإن

(أ) $aR\,p \quad \Leftrightarrow \quad a^{\frac{p-1}{2}} \equiv 1\ (\mathrm{mod}\ p)$.

(ب) $aN\,p \quad \Leftrightarrow \quad a^{\frac{p-1}{2}} \equiv -1\ (\mathrm{mod}\ p)$.

<u>البرهان :</u>

ضع $m = 1$ في مبرهنة (٦-٢-١) تحصل على النتيجة .

□

<u>مثال (٧) :</u>

إذا كان $p = 13$ ، فإن $2^{\frac{13-1}{2}} = 2^6 \equiv 12 \equiv -1 (\mathrm{mod}\ 13)$ ، وعليـــه فـــإن $2N_{13}$ أما $3^6 = (3^3)^2 \equiv 1^2 \equiv 1 (\mathrm{mod}\ 13)$ ، وعليه فإن $3R_{13}$ ، بينما $4R_{13}$ لأن $4^6 \equiv 2^{12} \equiv 1 (\mathrm{mod}\ 13)$.

<u>مثال (٨) :</u>

إذا كـــان $n = 5^2 = 25$ ، فـــإن $\frac{p(p-1)}{2} = 10$, $2^{10} \equiv -1 (\mathrm{mod}\ 25)$ ، $3^{10} \equiv -1 (\mathrm{mod}\ 25)$ ، وعليـــه فـــإن $3N_{25}, 2N_{25}$ بينمـــا $4R25$ لأن $4^{10} \equiv 1 (\mathrm{mod}\ 25)$ كما أن $11\,R25$ ، لأن $(11)^{10} \equiv 1 (\mathrm{mod}\ 25)$.

والآن إلى تعريف رمز لجندر ودراسة خواصه .

تعريف ٦-٢-٢ : (لجندر ١٧٩٨)

إذا كان p عدداً أولياً فردياً و $(a,p)=1$ ، فيعرّف رمز لجندر (Legendre Symbol) (a/p) كالآتي :

$$(a/p)=\begin{cases} 1 & aRp \quad \text{إذا كان} \\ -1 & aNp \quad \text{إذا كان} \\ 0 & a\equiv 0 \bmod p \quad \text{إذا كان} \end{cases}$$

مثال (٩) :

(أ) إذا كان $p=7$ ، فإن $(1/7)=(2/7)=(4/7)=1$ ، لأن كلاً من 1,2,4 باقي تربيعي قياس 7 . أما $(3/7)=(5/7)=(6/7)=-1$ ، لأن كلاً من 3,5,6 باقي غير تربيعي قياس 7 .

(ب) إذا كان $p=11$ ، فإن

$(1/11)=(3/11)=(4/11)=(5/11)=(9/11)=1$ ، لأن aR_{11} عندما $a=1,3,4,5,9$. أما

$(2/11)=(6/11)=(7/11)=(8/11)=(10/11)=-1$ ، لأن aN_{11} عندما $a=2,6,7,8,10$.

مبرهنة ٦-٢-٢ :

إذا كان p عدداً أولياً فردياً وكان $a,b\in Z$ ، $(a,p)=(b,p)=1$ ، فإن

(أ) $(a/p)\equiv a^{\frac{p-1}{2}} \pmod p$

(ب) إذا كان $a\equiv b \pmod p$ ، فإن $(a/p)=(b/p)$.

(ج) $(a^2/p)=1$. ، (د) $(ab/p)=(a/p)(b/p)$.

(هـ) $(1/p)=1$, $(-1/p)=(-1)^{\frac{p-1}{2}}$ ، (و) $(ab^2/p)=(a/p)$.

البرهان :

(أ) بتطبيق مبرهنة (٦-٢-١) أو نتيجتها نجد أن $(a/p) \equiv a^{\frac{p-1}{a^2}} \pmod p$.

(ب) بما أن $a \equiv b \pmod p$ إذاً إذا وجد حل لكل من $x^2 \equiv a \pmod p$ و $x^2 \equiv b \pmod p$ ، فإن لكل منهما نفس الحلول وعليه أما لكل من $x^2 \equiv a \pmod p$ ، $x^2 \equiv b \pmod p$ حل أو ليس لكل منهما حل . إذاً $(a/b) = (b/p)$.

(ج) بما أن a حل للعلاقة $x^2 \equiv a^2 \pmod p$. إذاً $(a^2/p) = 1$.

(د) بما أن $(ab/p) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod p \equiv (a/p)(b/p)$ حسب (أ) . وبما أن لرمز لجندر القيم 1 أو -1 . إذاً إذا كان $(ab/p) \neq (a/p)(b/p)$ ، فإن $1 \equiv -1 \pmod p$ ، وعليه فإن $2 \equiv 0 \pmod p$ ، ومنها نجد أن $p = 2$ وهذا يناقض كون p عدداً أولياً فردياً . إذاً $(ab/p) = (a/p)(b/p)$.

(هـ) بما أن $(1, p) = 1$. إذاً بوضع $a = 1$ في (ج) ، نجد أن $(1/p) = 1$ ، وبوضع $a = -1$ في (أ) نجد أن $(-1/p) \equiv (-1)^{\frac{p-1}{2}} \pmod p$. لكن إذا كان $(-1/p) = 1$ ، فإن $(-1)^{\frac{p-1}{2}} = 1$. وإذا كان $(-1/p) = -1$ ، فإن $(-1)^{\frac{p-1}{2}} = -1$ ، وعليه فإن $(-1/p) = (-1)^{\frac{p-1}{2}}$.

(و) بما أن $(ab^2/p) = (a/p)(b^2/p)$ حسب (د) ، وبما أن $(b^2/p) = 1$ حسب (ج) . إذاً $(ab^2/p) = (a/p)$. □

نتيجة : إذا كان p عدداً أولياً فردياً ، فإن

$$(-1/p) = \begin{cases} 1 & p \equiv 1 \pmod 4 \text{ إذا كان} \\ -1 & p \equiv 3 \pmod 4 \text{ إذا كان} \end{cases}$$

البرهان :

إذا كان $p = 4m + 1$ ، فإن $\frac{p-1}{2} = 2m$ عدد زوجي . لكن $(-1/p) = (-1)^{\frac{p-1}{2}}$ حسب مبرهنة (٦-٢-٢هـ) . إذاً $(-1/p) = (-1)^{2m} = 1$. أما إذا كان $p = 4m + 3$ ، فإن $\frac{p-1}{2} = 2m + 1$ عدد فردي ، وعليه فإن $(-1/p) = (-1)^{2m+1} = -1$.

□

وكتطبيق للمبرهنة (٦-٢-٢) ونتيجتها نورد ما يلي .

مثال (١٠) :

أثبت أن للتطابق $x^2 \equiv -38 \pmod{17}$ حل .

الإثبات :

بما أن $p = 17 = 4 \cdot 4 + 1$. إذاً $(-1/p) = 1$ حسب نتيجة مبرهنة (٦-٢-٢)، وعليه فإن $(-38/17) = (-1/17)(38/17) = (38/17)$. لكن $38 \equiv 4 \pmod{17}$. إذاً $(38/17) = (4/17)$ حسب مبرهنة (٦-٢-٢ب) . لكن $(4/17) = (2^2/17) = 1$ حسب مبرهنة (٦-٢-٢ج) . إذاً $(38/17) = 1$، وعليه فإن $38 R_{17}$ وبالتالي فإن للتطابق $x^2 \equiv -38 \pmod{17}$ حل .

مثال (١١) :

برهن على عدم وجود أعداد صحيحة x, y بحيث أن $y^2 = x^3 + 11$.

الإثبات :

نفرض وجود $x, y \in Z$ بحيث أن $y^2 = x^3 + 11$. إذاً $y^2 = x^3 + 11 \pmod{4}$ ، وعليه فإن $y^2 \equiv x^3 + 3 \pmod{4}$ ، ومنه نجد أن $x^3 + 3 \equiv 0 \pmod{4}$ ، وبالتالي فإن $x^3 \equiv -3 \equiv 1 \pmod{4}$ وعليه فإن $x \equiv 1 \pmod{4}$. إذاً $y^2 + 16 = x^3 + 27 = (x+3)(x^2 - 3x + 9)$. لكن

$x \equiv 1 \pmod 4$. إذاً $x^2 - 3x + 9x \equiv 3 \pmod 4$ ، وعليه يوجد عدد أولي $p \equiv 3 \pmod p$ و $x^2 - 3x + 9 \equiv 0 \pmod p$ ، وبالتالي فإن $y^2 + 16 \equiv 0 \pmod p$ ، ومنها نجد أن $\frac{y^2}{16} + 1 \equiv 0 \pmod p$ ، وعليه فإن $(\frac{y}{4})^2 \equiv -1 \pmod p$. إذاً $\left((\frac{y^2}{4})^2 \big/ p \right) = (-1/p)$ ، وعليه فإن $(-1/p) = 1$ و $p \equiv 3 \pmod 4$ وهذا يناقض نتيجة المبرهنة (٦-٢-٢) . إذاً لا يوجد $x, y \in Z$ بحيث أن $y^2 = x^3 + 11$.

والآن إلى المبرهنة الآتية التي تبين بأن عدد البواقي التربيعية قياس p يساوي عدد البواقي غير التربيعية قياس p ، كما توضح كيفية حسابها .

مبرهنة ٦-٢-٤ :

إذا كان p عدداً أولياً فردياً ، فإن $\sum_{a=1}^{p-1} (a/p) = 0$

البرهان :

ليكن r جذراً بدائياً قياس p . إذاً كل عنصر في $S = \{r, r^2, \ldots, r^{p-1}\}$ يطابق عنصراً وحيداً في $Z_p^* = \{1, 2, \ldots, p-1\}$ حسب مبرهنة (٦-١-٢) ، وعليه فإن لكل $1 < a < p-1$ يوجد عنصر وحيد k ، وحيث $1 \le k \le p-1$ بحيث أن $a \equiv r^k$ ، وبالتالي فإن $(a/p) = (r^k/p)$ حسب مبرهنة (٦-٢-٢ب) . لكن $(r^k/p) \equiv (r^k)^{\frac{p-1}{2}} = (r^{\frac{p-1}{2}})^k \pmod p$ حسب مبرهنة (٦-٢-٢أ) .

وحيث أن r جذر بدائي قياس p . إذاً $r^{\frac{p-1}{2}} \equiv -1 \pmod p$ ، وعليه فإن $(r^k/p) = (-1)^k$. إذاً $(a/p) = (-1)^k$ ، وعليه فإن

$$\sum_{a=1}^{p-1} (a/p) = \sum_{k=1}^{p-1} (-1)^k = 0$$

نستنتج من مبرهنة (٦-٢-٤) ، أنه إذا كان p عدداً فردياً أولياً وكان r جـذراً بدائياً إلى p ، فإن $r^{2m}(\text{mod } p)$ باقي تربيعي قياس p و $r^{2m+1}(\text{mod } p)$ باقي غير تربيعي قياس p ، حيث $m \in Z^+$.

□

مثال (١٢) :

إذا كان $p = 11$ ، فإن 2 جذر بدائي قياس 11 ، لأن $\text{ord}_{11}(2) = \phi(11) = 10$ ، وبالتالي فإن البواقي التربيعية قياس 11 هي

$$2^2 \equiv 4 \ , \ 2^4 \equiv 5 \ , \ 2^6 \equiv 9 \ , \ 2^8 \equiv 3 \ , \ 2^{10} \equiv 1 \pmod{11}$$

أما البواقي غير التربيعية قياس 11 فهي

$$2^1 \equiv 2 \ , 2^3 \equiv 5 \ , 2^5 \equiv 10 \ , 2^7 \equiv 7 \ , 2^9 \equiv 6 \pmod{11}$$

تمـــــارين

(١) أوجد البواقي التربيعية وغير التربيعية لكل من $13, 23, 29, 31$.

(٢) أوجد البواقي التربيعية لكل من $21, 25, 35, 105$.

(٣) حقق مبرهنة (٦-٢-٤) عندما $p = 13$ ، $p = 17$.

(٤) إذا كان 2 جذراً بدائياً إلى 19 ، فأوجد جميع البواقي التربيعية إلى 19 .

(٥) برهن على عدم وجود أعداد صحيحة x, y بحيث أن $y^2 = x^3 + 7$.

(٦) إذا كان p عدداً أولياً فردياً وكان aRp ، فأثبت أن :

(أ) a ليست جذراً بدائياً إلى p .

(ب) إذا كان $p \equiv 1 \pmod 4$ ، فإن $(p-a)R_p$.

(ج) إذا كان $p \equiv 3 \pmod 4$ ، فإن $(p-a)N_p$.

(٧) إذا كان $p = 2^n + 1$ عدداً أولياً ، وكان aN_p ، فأثبت أن a جذر بـــدائي إلى p " طبق مبرهنة (٦-٢-١) " .

(٨) إذا كان كل من p ، $q = 4p+1$ عدداً أولياً وكان aN_q ، فأثبت أن :

(أ) أما أن يكون a جذراً بدائياً إلى q أو أن $\text{ord}_q(a) = 4$.

"لاحظ أن aN_q يعني $-1 = (a/q) \equiv a^{2p} (\text{mod } q)$ ، وعليه فإن $\text{ord}_q(a) = 1, 2, 4, p, 2p, 4p$ " .

(ب) 2 جذر بدائي إلى q .

(٩) إذا كان $p > 3$ عدداً أولياً ، فأثبت أن

$$(-3/p) = \begin{cases} 1 & p \equiv 1 (\text{mod } 3) \quad \text{إذا كان} \\ -1 & p \equiv 2 (\text{mod } 3) \quad \text{إذا كان} \end{cases}$$

ثم أحسب $(-3/13)$ ، $(-3/19)$ ، $(-3/17)$ ، $(-3/23)$

(١٠) أحسب كلاً من

$$(2/13), (3/13), (7/13), (6/13)$$

٦-٣ : " قانون التعاكس الثنائي Quadratic Reciprocity Law "

ينص قانون التعاكس الثنائي على أنه " إذا كان p, q عددين أوليين مختلفين ، فأما لكلا التطابقين $x^2 \equiv p (\text{mod } q)$ و $x^2 \equiv q (\text{mod } p)$ حل أو ليس لكليهما حل بشرط أن p, q ليسا على الصورة $4k+3$. أما إذا كان كل منهما على الصورة $4k+3$ ، فإن لأحد التطابقين حل بينما لا يوجد حل للآخر " .

وقد خمّن أويلر قانون التعاكس سنة ١٧٤٢م نتيجة لبحثه عن القواسم الأولية للأعداد التي على الشكل $a^n \mp b^n$ ، ثم أعاد صياغته دون إثبات سنة ١٧٨٣م ، وقدم لجندر أثباتياً جزئياً (غير مكتمل) لذلك القانون سنة ١٧٨٥م ، ثم أعاد جاوس أكتشاف قانون التعاكس وهو في سن ١٨ سنة وأثبته سنة ١٧٩٦م ونشر البرهان سنة ١٨٠١م ، ثم قدم جاوس سبعة براهين أخرى لذلك القانون ، ويوجد اليوم 200 برهان لهذا القانون .

ولإثبات قانون التعاكس وتناول بعض تطبيقاته نورد الآتي :

مبرهنة ٦-٣-١: "Gauss Lemma"

إذا كان p عدداً أولياً فردياً و $a \in Z^+$ ، $(a,p)=1$ وكانت $A=\{a,2a,3a,\cdots,\frac{(p-1)a}{2}\}$ وكان n يمثل عدد عناصر A التي باقي قسمة كل منها على p أكبر من $\frac{p}{2}$ ، فإن $(a \setminus p)=(-1)^n$.

البرهان :

بما أن $(a,p)=1$. إذاً $x \not\equiv 0 (\text{mod } p)$ لكل $x \in A$ ، كما أن $x \not\equiv y (\text{mod } p)$ لكل $x,y \in A$.

والآن لنفرض أن $r_1,r_2,...,r_m$ هي بواقي قسمة عناصر A على p والتي تحقق العلاقة $0<r_i<p/2$ ، وأن $s_1,s_2...,s_n$ هي بواقي قسمة عناصر A على p والتي تحقق العلاقة $\frac{p}{2}<s_i<p$ إذاً $m+n=\frac{p-1}{2}$ ، كما أن $r_1,...,r_m \, , p-s_1,p-s_2,...,p-s_n$ أعداد صحيحة موجبة كل منها أقل من $\frac{p}{2}$.

والآن لنفرض أن $p-s_i=r_j$ لبعض قيم i,j. إذاً يوجد $u,v \in Z$ ، $1 \le u,v \le \frac{p-1}{2}$ ، بحيث أن $r_j=va(\text{mod } p)$ ، $s_i=ua(\text{mod } p)$ ، وعليه فإن $(u+v)a \equiv s_i+r_j=p\equiv 0(\text{mod } p)$. لكن $(a,p)=1$. إذاً $u+v\equiv 0(\text{mod } p)$ وهذا غير ممكن لأن $1<u+v\le p-1$. إذاً $p-s_i \ne r_j$ لكل i,j ، وبالتالي فإن

$$B=\{r_1,r_2,...,r_m \, , p-s_1,p-s_2,...,p-s_n\}=\{1,2,...,\frac{p-1}{2}\}$$

وعليه فإن

$$\left(\prod_{i=1}^{m} r_i\right)\left(\prod_{j=1}^{n}(p-s_j)\right)=1\cdot 2\cdots\frac{p-1}{2}=(\frac{p-1}{2})!$$

إذاً $\prod_{i=1}^{m} r_i \cdot \prod_{j=1}^{n}(-s_j) \equiv (\frac{p-1}{2})!(\text{mod } p)$ ، وعليه فإن

$$(-1)^n\left(\prod_{i=1}^{m} r_i\right)\left(\prod_{j=1}^{n} s_j\right) \equiv (\frac{p-1}{2})!(\text{mod } p)$$

لكن لكل $b \in B$ يوجد $c \in A$ بحيث أن $b \equiv c(\text{mod } p)$. إذاً $(-1)^n \cdot a \cdot 2a \cdot 3a \cdots (\frac{p-1}{2})a \equiv (\frac{p-1}{2})!\ (\text{mod } p)$ ، وعليه فإن $(-1)^n \cdot a^{\frac{p-1}{2}} \cdot (\frac{p-1}{2})! \equiv (\frac{p-1}{2})!\ (\text{mod } p)$. لكن $\left((\frac{p-1}{2})!, p\right) = 1$. إذاً $(-1)^n \cdot a^{\frac{p-1}{2}} \equiv 1\ (\text{mod } p)$ ، وعليه فإن $a^{\frac{p-1}{2}} \equiv (-1)^n\ (\text{mod } p)$. لكن $(a/p) \equiv a^{\frac{p-1}{2}}\ (\text{mod } p)$ حسب مبرهنة (٦-٢-٢أ) . إذاً $(a/p) = (-1)^n$.

□

مثال (١) : أحسب $(3/11)$ ، $(7/11)$.

الحل :

بما أن $5 = \frac{11-1}{2} = \frac{p-1}{2}$. إذاً عندما $a = 3$ ، نجد أن

$$A = \{3,6,9,12,15\}$$
$$= \{3(\text{mod } 11), 6(\text{mod } 11), 9(\text{mod } 11), 1(\text{mod } 11), 4(\text{mod } 11)\}$$

وعنصرين من عناصر A أكبر من $\frac{11}{2}$. إذاً $n = 2$ ، وعليه فإن $(3/11) = (-1)^2 = 1$.

أما عندما $a = 7$ ، فإن

$$A = \{7,14,21,28,35\}$$
$$= \{7(\text{mod } 11), 3(\text{mod } 11), 10(\text{mod } 11), 6(\text{mod } 11), 2(\text{mod } 11)\}$$

وثلاثة من عناصر A أكبر من $\frac{11}{2}$. إذاً $n = 3$ ، وعليه فإن $(7/11) = (-1)^2 = -1$.

ومن تطبيقات مبرهنة (٦-٣-١) ما يلي :

مبرهنة ٦-٣-٢ :

إذا كان p عدداً أولياً فردياً ، فإن

$$(2/p)=\begin{cases}1 & p\equiv \mp 1 \pmod 8 \text{ إذا كان } \\ -1 & p\equiv \mp 3 \pmod 8 \text{ إذا كان }\end{cases}$$

البرهان :

بما أن $a=2$. إذاً $A=\{1,4,6,\cdots,p-1\}$. ولحساب n ، لاحظ أن p عدد فردي . إذاً $p=4m+1$ ، $p=4m+3$.

فإذا كان $p=4m+1$ ، فإن

$$\{x\in A \mid x=tp+r, r>p/2\}$$
$$=\left\{x\in A \mid x=(\frac{p-1}{2})+2k, k=1,\cdots,\frac{p-1}{4}\right\}$$

وعليه فإن $n=\dfrac{p-1}{4}$. لكن $(2/p)=(-1)^n$ حسب مبرهنة (٦-٣-١) . إذاً

$$(2/p)=(-1)^{\frac{p-1}{4}}=\begin{cases}1 & p\equiv 1 \pmod 8 \text{ إذا كان } \\ -1 & p\equiv -3 \pmod 8 \text{ إذا كان }\end{cases}$$

أما إذا كان $p=4m+3$

$$\{x\in A \mid x=tp+r, r>p/2\}$$
$$=\left\{x\in A \mid x=(\frac{p-1}{2})+2k-1, k=1, 2,\cdots,\frac{p+1}{4}\right\}$$

وعليه فإن $n=\dfrac{p+1}{4}$ ، وبالتالي فإن

$$(2/p)=(-1)^{\frac{p+1}{4}}=\begin{cases}1 & p\equiv -1 \pmod 8 \text{ إذا كان } \\ -1 & p\equiv 3 \pmod 8 \text{ إذا كان }\end{cases}$$

إذاً

$$(2/p)=\begin{cases}1 & p\equiv \mp 1 \pmod 8 \text{ إذا كان } \\ -1 & p\equiv \mp 3 \pmod 8 \text{ إذا كان }\end{cases}$$

نتيجة (١) :

إذا كان p عدداً أولياً فردياً ، فإن $(2/p)=(-1)^{\frac{p^2-1}{8}}$

البرهان :

بما أن

$$(2/p)=\begin{cases}1 & p\equiv\mp1 \pmod 8 \quad \text{إذا كان}\\ -1 & p\equiv\mp3 \pmod 8 \quad \text{إذا كان}\end{cases}$$ حسب مبرهنة (٦-٣-٢) .

إذاً ، إذا كان $p=8m\mp1$ ، فإن

$$\frac{p^2-1}{8}=\frac{(8m\mp1)^2-1}{8}=8m^2\mp2m$$

وعليه فإن $\frac{p^2-1}{8}$ عدد زوجي ، وبالتالي فإن $1=(-1)^{\frac{p^2-1}{8}}$.

أما إذا كان $p=8m\mp3$ ، فإن

$\frac{p^2-1}{8}=8m^2\mp6m+1$ عدد فردي ، وعليه فإن $-1=(1)^{\frac{p^2-1}{8}}$. إذاً

$$(2/p)=(-1)^{\frac{p^2-1}{8}}$$

□

نتيجة (٢) :

إذا كان $p=(2q+1)\equiv-1 \pmod 8$ عدداً أولياً، فإن p/M_q .

البرهان :

بما أن $p\equiv-1 \pmod 8$. إذاً $(2/p)=1$ حسب مبرهنة (٦-٣-٢) . لكن $(2/p)\equiv2^{\frac{p-1}{2}} \pmod p$ حسب نتيجة مبرهنة (٦-٢-١) . إذاً $2^{\frac{p-1}{2}}\equiv1 \pmod p$. لكن $2^{\frac{p-1}{2}}=2^q$ ، إذاً $2^q\equiv1 \pmod p$ ، وعليه فإن $p\backslash(2^q-1)$. لكن $M_q=2^2-1$. إذاً p/M_q .

□

مثال (٢) :

(أ) $167 \setminus M_{83}$ ، لأن $167 = 2(83) + 1 \equiv -1 (\mod 8)$ عدد أولي .

(ب) $359 \setminus M_{179}$ ، لأن $359 = (2 \cdot 179 + 1) \equiv -1 (\mod 8)$ عدد أولي .

(ج) $151 \setminus M_{75}$ ، لأن $151 = (75) + 1 \equiv -1 (\mod 8)$ عدد أولي .

مبرهنة ٦-٣-٣ :

إذا كان كل من $p, 2p+1$ عدداً أولياً فردياً ، فإن $2(-1)^{\frac{p-1}{2}}$ جذر بدائي إلى $2p+1$.

البرهان :

نفرض أن $q = 2p + 1$. بما أن p عدد فردي . إذاً $p \equiv 1 (\mod 4)$ أو $p \equiv 3 (\mod 4)$.

(أ) إذا كان $p \equiv 1 (\mod 4)$ ، فإن $2(-1)^{\frac{p-1}{2}} = 2$ لكن $\phi(q) = 2p$. إذاً $\text{ord}_q(2) = 1, 2, p, 2p$. فإذا كان $\text{ord}_q(2) = 1$ ، فإن ذلك يعني أن $2 \equiv 1 (\mod q)$ ، وبالتالي فإن $q \setminus 1$ وهذا غير ممكن . إذاً $\text{ord}_q(2) \neq 1$. وإذا كان $\text{ord}_q(2) = 2$ ، فإن $2^2 \equiv 1 (\mod q)$ ، وعليه فإن $q \setminus 3$ وهذا غير ممكن لأن $q = 2p + 1$. إذاً $\text{ord}_q(2) \neq 2$.

وحيث أن $(2/q) = 2^{\frac{q-1}{2}} = 2^p (\mod q)$ حسب مبرهنة (٦-٢-٢أ) و $q = 2p + 1 \equiv 3 (\mod 8)$. إذاً $(2/p) = -1$ مبرهنة (٦-٣-٢) ، وعليه فإن $2^p \equiv -1 (\mod q)$ ، وبالتالي فإن $\text{ord}_q(2) \neq p$. إذاً $\text{ord}_q(2) = 2p$ ، وعليه فإن 2 جذر بدائي إلى q .

(ب) إذا كان $p \equiv 3 (\mod 4)$ ، فإن $2(-1)^{\frac{p-1}{2}} = -2$ و $(-2)^p \equiv (-2/q) = (-1/q)(2/q)$. لكن $q = 2p + 1$. إذاً

$q \equiv 3 \pmod 4$ ، وعليه فإن $(-1/q) = -1$ حسب نتيجة مبرهنة (٦-٢-٢) و $(2/q) = 1$ حسب مبرهنة (٦-٣-٢) ، وبالتالي فإن $(-2)^p \equiv -1 \pmod q$ ، وعليه فإن $ord_q(-2) \neq p$.

وإذا كان $ord_q(2) = 1,2$ ، فإن ذلك يعني أن $q \setminus 3$ وهذا غير ممكن .

إذاً $ord_q(-2) \neq 1,2$ ، وعليه فإن $ord_q(-2) = 2p = \phi(q)$ ، وبالتالي فإن -2 جذر بدائي إلى q .

□

مثال (٣) :

(أ) 2 جذر بدائي إلى 179 ، لأن $179 = 2(89) + 1$ وكل من 89,179 عدد أولي فردي ، كما أن $2(-1)^{\frac{p-1}{2}} = 2(-1)^{44} = 2$.

(ب) -2 جذر بدائي إلى 167 ، لأن $167 = 2(83) + 1$ وكل 83,167 عدد أولي فردي و $2(-1)^{\frac{p-1}{2}} = 2(-1)^{\frac{83-1}{2}} = 2(-1)^{41} = -2$.

وقبل إثبات المبرهنة الآتية ، لاحظ أن [x] يمثل أكبر عدد صحيح أصغر من أو يساوي x .

مبرهنة ٦-٣-٤ :

إذا كان p عدد فردياً أولياً ، وكان a عدداً فردياً ، $(a,p) = 1$ ، فإن

$$(a/p) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} [ka/p]}$$

البرهان :

لتكن $A = \{a, 2a, \cdots, (\frac{p-1}{2})a\}$. إذاً أي عنصر من عناصر A على الشكل ka . وبقسمة ka على p نجد أن $ka = q_k \cdot p + t_k$ ، حيث $1 \leq t_k \leq p-1$ وعليه فإن $ka/p = q_k + (t_k/p)$ ، ومنها نجد أن $[ka/p] = q_k$

وعليه إذا كان $1 \le k \le \frac{p-1}{2}$ ، فإن

$$ka = [ka/p] + t_k \qquad \ldots(1)$$

والآن لتكن $B = \{r_1, r_2, \cdots, r_m\}$ مجموعة بواقي قسمة عناصر A على p التي تحقق العلاقة $0 < r_i < p/2$ ، ولتكن $C = \{s_1, \cdots, s_n\}$ مجموعة بـواقي قسمة عناصر A على p التي تحقق العلاقة $\frac{p}{2} < s_i < p$. إذاً $t_k < p/2$ يعني أن $t_k \in B$. أما إذا كان $t_k > p/2$ ، فإن $t_k \in C$ ، وعليه من (1) نجد أن

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} [ka/p] + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k \qquad \ldots(2)$$

لكن $D = \{r_1, \cdots, r_m , p - s_1, p - s_2, \cdots, p - s_m\} = \{1, 2, \cdots, \frac{p-1}{2}\}$. إذاً

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = p \cdot n + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k \qquad \ldots(3)$$

وبطرح (3) من (2) نجد أن

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} k = p\left(\sum_{k=1}^{\frac{p-1}{2}} [ka/p] - n \right) + 2\sum_{k=1}^{n} s_k$$

لكن $p \equiv a \equiv 1 (\mathrm{mod}\ 2)$. إذاً $a - 1 \equiv 0 (\mathrm{mod}\ 2)$ ، وعليه فإن

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} k \equiv 0 (\mathrm{mod}\ 2)$$

وبالتالي فإن $\sum_{k=1}^{\frac{p-1}{2}} \left([ka/p] - n \right) \equiv 0 (\mathrm{mod}\ 2)$ ، ومنها نجد أن

$$\sum_{k=1}^{\frac{p-1}{2}} [ka/p] \equiv n$$

لكن $(a/p) = (-1)^n$ حسب مبرهنة (٦-٣-١). إذاً

$$(a/p) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} [ka/p]}$$

□

والآن إلى قانون التعاكس والمبرهنة الآتية .

مبرهنة ٦-٣-٥ : "قانون التعاكس لجاوس"

إذا كان p,q عددين أوليين فرديين مختلفين ، فإن

$$(p/q)(q/p)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

البرهان :

لتكن

$$S=\{(x,y)\in Z^2 \ \left|1\le x\le \frac{p-1}{2}, 1\le y\le \frac{q-1}{2}\right.\}$$

إذاً لا يوجد $(x,y)\in S$ بحيث $qx=py$ ، وعليه يمكن تجزئة S إلى مجموعتين S_1, S_2 ، حيث

$$S_1=\{(x,y)\in S \ |qx>py\}, S_2=\{(x,y)\in S \ |qx<py\}$$

إذاً

$$(x,y)\in S_1 \Leftrightarrow 1\le x\le \frac{p-1}{2}, 1\le y\le [qx/p]$$

وعليه فإن

$$|S_1|=\sum_{x=1}^{\frac{p-1}{2}}[qx/p]$$

وبالمثل نجد أن $|S_2|=\sum_{y=1}^{\frac{q-1}{2}}[py/q]$ ، وبالتالي فإن

$$\sum_{x=1}^{\frac{p-1}{2}}[qx/p]+\sum_{x=1}^{\frac{q-1}{2}}[py/q]=|S_1|+|S_2|=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

لكن

$$(q/p)=(-1)^{\sum_{y=1}^{\frac{q-1}{2}}[py/q]} \text{ ، } (p/q)=(-1)^{\sum_{x=1}^{\frac{p-1}{2}}[qx/p]}$$

حسب مبرهنة (٦-٣-٤) . إذاً $(p/q)\,(q/p)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

نتيجة (١) :

إذا كان p,q عددين أوليين فرديين مختلفين ، فإن

$$(p/q)\,(q/p)=\begin{cases}1 & \text{إذا كان } q\equiv 1(\text{mod } 4) \text{ أو } p\equiv 1(\text{mod } 4)\\ -1 & \text{إذا كان } p\equiv q\equiv 3(\text{mod } 4)\end{cases}$$

البرهان :

بما أن p,q عددان فرديان . إذاً $\frac{p-1}{2}\cdot\frac{q-1}{2}$ عدد زوجي إذاً وإذا فقط كان واحد على الأقل من العددين p, q على الشكل $4k+1$ ، وعليه فإن

$$(p/q)\,(q/p)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=1$$

أما إذا كان $p\equiv q\equiv 3(\text{mod } 4)$ ، فإن $\frac{p-1}{2}\cdot\frac{q-1}{2}$ عدد فردي ، وعليه فإن

$$(p/q)\,(q/p)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=-1$$

□

نتيجة (٢) :

إذا كان p,q عددين أوليين فرديين مختلفين ، فإن

$$(p/q)=\begin{cases}(q/p) & \text{إذا كان } q\equiv 1(\text{mod } 4) \text{ أو } p\equiv 1(\text{mod } 4)\\ -(q/p) & \text{إذا كان } p\equiv q\equiv 3(\text{mod } 4)\end{cases}$$

البرهان :

إذا كان $p\equiv 1(\text{mod } 4)$ أو $q\equiv 1(\text{mod } 4)$ ، فإن $(p/q)\,(q/p)=1$ حسب نتيجة (١) . وعليه فإن $(p/q)\,(q/p)^2=(q/p)$. لكن $(q/p^2)=1$ إذاً $(p/q)=(q/p)$.

أما إذا كان $p\equiv q\equiv 3(\text{mod } 4)$ ، فإن $(p/q)\,(q/p)=-1$ حسب نتيجة (١) ، وعليه فإن $(p/q)\,(q/p)^2=-(q/p)$ ، وبالتالي فإن $(p/q)=-(q/p)$. إذاً

$$(p/q)=\begin{cases}(q/p) & \text{إذا كان } q\equiv 1(\text{mod } 4) \text{ أو } p\equiv 1(\text{mod } 4)\\ -(q/p) & \text{إذا كان } p\equiv q\equiv 3(\text{mod } 4)\end{cases}$$

مبرهنة ٦-٣-٦ :

إذا كان $p \neq 3$ عدداً أولياً فردياً ، فإن

$$(3/p) = \begin{cases} 1 & p \equiv \mp 1 \pmod{12} \text{ إذا كان } \\ -1 & p \equiv \mp 5 \pmod{12} \text{ إذا كان } \end{cases}$$

البرهان :

بما أن $3 \equiv 3 \pmod 4$. إذاً بتطبيق نتيجة (٢) من مبرهنة (٦-٣-٥) نجد أن

$$(3/p) = \begin{cases} (p/3) & p \equiv 1 \pmod 4 \text{ إذا كان } \\ -(p/3) & p \equiv 3 \pmod 4 \text{ إذا كان } \end{cases} \quad \ldots (1)$$

وبتطبيق قانون التعاكس نجد أن

$$(-3/p) = (-1/p)(3/p) = (-1)^{\frac{p-1}{2}} (p/3)(-1)^{\frac{(3-1)p-1)}{4}}$$
$$= (-1)^{p-1} \cdot (p/3) = (p/3)$$

وعليه فإن

$$(p/3) = (-3/p) = \begin{cases} 1 & p \equiv 1 \pmod 3 \text{ إذا كان } \\ -1 & p \equiv 2 \pmod 3 \text{ إذا كان } \end{cases} \quad \ldots (2)$$

ومن (1) ، (2) نجد أن

$$(3/p) = 1 \Leftrightarrow \left(p \equiv 1 \pmod 4 \wedge p \equiv 1 \pmod 3 \right)$$
$$\vee \left(p \equiv 3 \pmod 4 \wedge p \equiv 2 \pmod 3 \right)$$
$$\Leftrightarrow p \equiv 1 \pmod{12} \vee \left(p \equiv 3 \equiv -1 \pmod 4 \wedge p \equiv 2 \equiv -1 \pmod 3 \right)$$
$$\Leftrightarrow p \equiv 1 \pmod{12} \vee p \equiv -1 \pmod{12}$$
$$(3/p) = -1 \Leftrightarrow \left(p \equiv 1 \pmod 4 \wedge p \equiv 2 \pmod 3 \right)$$
$$\vee \left(p \equiv 1 \pmod 3 \wedge p \equiv 3 \pmod 4 \right)$$
$$\Leftrightarrow \left(p \equiv 5 \pmod 4 \wedge p \equiv 5 \pmod 3 \right)$$
$$\vee \left(p \equiv -5 \pmod 3 \wedge p \equiv -5 \pmod 4 \right)$$
$$\Leftrightarrow p \equiv 5 \pmod{12} \vee p \equiv -5 \pmod{12}$$

وعليه فإن $(p/3)=\begin{cases} 1 & p\equiv \mp 1(\text{mod } 12) \text{ إذا كان} \\ -1 & p\equiv \mp 5(\text{mod } 12) \text{ إذا كان} \end{cases}$

□

والآن إلى بعض التطبيقات والأمثلة الآتية .

مثال (٤) : أحسب

(أ) $(41/89)$ ، (ب) $(69/389)$

الحل :

(أ) $89\equiv 1(\text{mod } 4), 41\equiv 1(\text{mod } 4)$ وكل من $41,89$ عدد أولي فردي إذاً $(41/89)=(89/41)$ حسب نتيجة (٢) مبرهنة (٦-٣-٥) لكن $89\equiv 7(\text{mod } 41)$. إذاً $(89/41)=(7/41)$ حسب مبرهنة(٦-٢-٢ب) لكن $(7/41)=(41/7)$ حسب نتيجة (٢) مبرهنة (٦-٣-٥) . كما أن $41\equiv 6(\text{mod } 7)$. إذاً $(41/7)=(6/7)$ ، وعليه فإن $(7/41)=(6/7)=(2/7)(3/7)$. لكن $(3/7)=-1$ حسب مبرهنة (٦-٣-٦) ، $(2/7)=1$ حسب مبرهنة (٦-٣-٢) . إذاً $(41/89)=1(-1)=-1$.

(ب) $(69/389)=(3.23/389)=(3/389)(23/389)$. لكن $389\equiv 5(\text{mod } 12)$. إذاً $(3/389)=-1$ حسب مبرهنة (٦-٣-٦) وحيث أن $389\equiv 1(\text{mod } 4)$. إذاً $(23/389)=(389/23)$ حسب نتيجة (٢) مبرهنة (٦-٣-٥) . لكن $389\equiv -2(\text{mod } 23)$. إذاً $(389/23)=(-2/23)$ حسب مبرهنة (٦-٢-٢ب) . لكن $(-2/23)=(-1/23)(2/23)$ و $(-1/23)=(-1)^{\frac{23-1}{2}}=-1$ حسب مبرهنة (٦-٢-٢هـ) ، $(2/23)=1$ حسب مبرهنة (٦-٣-٢) . إذاً $(-2/23)=-1$ ، وعليه فإن $(69/389)=(-1)(-1)=1$.

مثال (٥) :

أثبت أن 3 جذر بدائي إلى 17 .

الإثبات :

بما أن $17 \equiv 5 \pmod{12}$ ، إذاً $(3/17) = -1$ حسب مبرهنة (٦-٣-٦) .
لكن $(3/17) \equiv 3^{\frac{17-1}{2}} = 3^8 \pmod{17}$ حسب نتيجة مبرهنة (٦-٢-١) . إذاً $3^8 \equiv -1 \pmod{17}$ ، وبالتالي فإن $3^{16} \equiv 1 \pmod{17}$. لكن $\phi(17) = 16$ إذاً $ord_{17}(3) = \phi(17)$ ، وعليه فإن 3 جذر بدائي إلى 17 .

مثال (٦) :

أثبت أن للتطابق $x^2 \equiv 5 \pmod{227}$ حل .

الإثبات :

بما أن للتطابق $x^2 \equiv a \pmod{p}$ حل إذاً وإذا فقط كان $(a/p) = 1$.
وبما أن $(5/227) = (227/5) = (2/5) = 1$. إذاً للتطابق $x^2 \equiv 5 \pmod{227}$ حل .

مثال (٧) :

هل للتطابق $x^2 \equiv 17 \pmod{299}$ حل ؟

الحل :

بما أن $299 = 13 \cdot 23$. إذاً للتطابق $x^2 \equiv 17 \pmod{299}$ حل إذاً وإذا فقط كان للتطابقين $x^2 \equiv 17 \pmod{23}$ و $x^2 \equiv 17 \pmod{13}$ حل . لكن $(17/23) = (23/17) = (6/17) = (2/17)(3/17) = 1(-1) = -1$. إذاً ليس للتطابق $x^2 \equiv 17 \pmod{23}$ حل . وعليه لا يوجد للتطابق $x^2 \equiv 17 \pmod{299}$ حل .

وأخيراً إلى تعريف رمز جاكوبي نسبة للرياضي الألماني (١٨٠٤-١٨٥١) ، ودراسة خواصه .

تعريف ٦-٣-١:

إذا كان $a,n \in \mathbb{Z}$ وكان n عدداً فردياً موجباً ، $n=\prod_{i=1}^{r} p_i$ ، حيث p_i أعداد فردية أولية ، فيعرف رمز جاكوبي (Jacobi Symbol) كالآتي :

$(a/n)=\prod_{i=1}^{r}(a/p_i)$ ، حيث أن (a/p_i) رمز لجندر .

لاحظ أن : (أ) $(a/n)=0 \Leftrightarrow (a,n)>1$.

(ب) $(a/1)=1$ لكل $a \in \mathbb{Z}$.

مثال (٨) :

(أ) $(3/35)=(3/5)(3/7)$. لكن $5 \equiv 5 \pmod{12}$ و$7 \equiv -5 \pmod{12}$

إذاً $(3/5)=-1$ ، $(3/7)=-1$ حسب مبرهنة (٦-٣-٦) ، وعليه فإن

$(3/35)=(-1)(-1)=1$.

(ب) $(6/385)=(6/5\cdot 7\cdot 11)=(6/5)(6/7)(6/11)$

$=(2/5)(3/5)(2/7)(3/7)(2/11)(3/11)$

حسب مبرهنة (٦-٢-٤هـ) . لكن $5 \equiv -3 \pmod 8$ ،

$7 \equiv -1 \pmod 8$ ، $11 \equiv 3 \pmod 8$. إذاً $(2/5)=-1$ ،

$(2/7)=1$ ، $(2/11)=-1$ حسب مبرهنة (٦-٣-٢) . وحيث أن

$5 \equiv 5 \pmod{12}$ ، $7 \equiv -5 \pmod{12}$ ، $11 \equiv -1 \pmod{12}$. إذاً

$(3/5)=-1$ ، $(3/7)=-1$ ، $(3/11)=1$ حسب مبرهنة (٦-٣-٦) ،

وعليه فإن

$$(6/385)=(-1)(-1)(1)(-1)(-1)(1)=1$$

مبرهنة ٦-٣-٧ :

إذا كان m,n عددين موجبين فرديين ، وكان $a,b \in \mathbb{Z}$ ، فإن

(أ) $(ab/n)=(a/n)(b/n)$ ، (ب) $(a,mn)=(a/m)(a/n)$

(ج) إذا كان $a \equiv b \pmod{n}$ ، فإن $(a/n) = (a/n)$.

(د) $(-1/n) = (-1)^{\frac{n-1}{2}}$ ، (هـ) $(m/n)(n/m) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$

(و) $(2/n) = (-1)^{\frac{n^2-1}{8}}$.

البرهان :

سنبرهن (د) ، (هـ) ، (و) ونترك الباقي للقارئ .

(د) نفرض أن $n = \prod_{i=1}^{r} p_i$ ، إذاً

$$(-1/n) = \prod_{i=1}^{r} (-1/p_i) = (-1)^{\sum_{i=1}^{r}(\frac{p_i-1}{2})}$$

لكننا يمكن أن نبرهن بالأستقراء على r ، أن

$\sum_{i=1}^{r}(\frac{p_i-1}{2}) \equiv \frac{n-1}{2} \pmod{2}$. إذاً $(-1/n) = (-1)^{\frac{n-1}{2}}$

(هـ) نفرض أن $m = \prod_{i=1}^{r} p_i$ ، $n = \prod_{j=1}^{s} q_j$. إذاً

$$(m/n)(n/m) = \prod_{i=1}^{r}\prod_{j=1}^{s} (p_i/q_j)\,(q_j/p_i)$$

$$= \prod_{i=1}^{r}\ \prod_{j=1}^{s}(-1)^{\frac{(p_i-1)(q_j-1)}{4}} = (-1)^{\sum_{i=1}^{s}\sum_{i=1}^{r}(\frac{p_i-1}{2})(\frac{q_j-1}{2})}$$

(حسب مبرهنة (٦-٣-٥) . لكن

$$\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2} = \sum_{i=1}^{r}\frac{p_i-1}{2}\cdot\sum_{j=1}^{s}\frac{q_j-1}{2}$$ و

$\sum_{i=1}^{r}\frac{p_i-1}{2} \equiv \frac{n-1}{2} \pmod{2}$ ، $\sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{m-1}{2} \pmod{2}$. إذاً

$$(m/n)(n/m) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$$

(و) إذا كان a,b عددين فرديين ، فإن

$$\frac{(ab)^2-1}{8}-(\frac{a^2-1}{8}+\frac{b^2-1}{8})=\frac{(a^2-1)(b^2-1)}{8}\equiv 0 \pmod 8$$

وعليه فإن $\frac{(ab)^2-1}{8}\equiv(\frac{a^2-1}{8}+\frac{b^2-1}{8}) \pmod 2$ ، إذاً

$\sum_{i=1}^{r}\frac{p_i^2-1}{8}\equiv\frac{n^2-1}{8} \pmod 2$ ، وعليه فإن

$$(2/n)=\prod_{i=1}^{r}(2/p_i)=(-1)^{\sum_{i=1}^{r}\frac{p_i^2-1}{8}}=(-1)^{\frac{n^2-1}{8}}$$

□

تمـــــارين

(١) أحسب كلاً مما يأتي :

$(-42/89)$, $(30/71)$ ، $(-56/103)$ ، $(15/107)$ ،
$(-219/383)$, $(21/221)$, $(3/97)$, $(22/11)$, $(51/7)$.

(٢) أحسب (p/q) عندما $p=7,11,13$ ، $q=227,229,1009$.

(٣) بتطبيق مبرهنة (٦-٣-١) أحسب كلاً مما يأتي
$(23/41)$, $(6/31)$, $(5/19)$, $(8/17)$.

(٤) (أ) أثبت أن $143 \setminus M_{71}$ ، $179 \setminus M_{89}$ ، $227 \setminus M_{113}$.
(ب) أثبت أن $M_n=2^n-1$ عدد مؤلف عندما
$n=11,23,131,239,251$.

(٥) أثبت بتطبيق مبرهنة (٦-٣-٣) أن :
(أ) 2 جذر بدائي لكل من $107,227,467$.
(ب) -2 جذر بدائي لكل من $47,143,263$.

(٦) لأي من علاقات التطابق الآتية حل ؟

(أ) $x^2 \equiv 5 \pmod{313}$ ، (ب) $x^2 \equiv 7 \pmod{1009}$

(ج) $x^2 \equiv 121 \pmod{413}$ ، (د) $x^2 \equiv 42 \pmod{97}$

(هـ) $x^2 \equiv -43 \pmod{79}$ ، (و) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$

(٧) إذا كان p عدداً أولياً فردياً ، فأثبت أن

$$(-2/p) = \begin{cases} 1 & \text{إذا كان } p \equiv 1 \pmod 8 \text{ أو } p \equiv 3 \pmod 8 \\ -1 & \text{إذا كان } p \equiv 5 \pmod 8 \text{ أو } p \equiv -1 \pmod 8 \end{cases}$$

(٨) أوجد جميع الأعداد الأولية التي تحقق :

(أ) $(5/p)$ ، (ب) $(10/p) = 1$

(٩) إذا كان $p = 2^{4n} + 1$ عدداً أولياً ، فأثبت أن 7 جذر بدائي إلى p .

"لاحظ أن $p \equiv 5 \pmod 7$ أو $p \equiv 3 \pmod 7$ وبالتالي فإن

$(7/p) = (p/p) = -1$ " .

(١٠) (أ) إذا كان p عدداً أولياً فردياً أكبر من 3 ، فأثبت أن :

$$(-3/p) = \begin{cases} 1 & p \equiv 1 \pmod 6 \\ -1 & p \equiv 5 \pmod 6 \end{cases}$$

(ب) أستخدم (أ) لإثبات وجود عدد غير منتهي من الأعداد الأولية التي على الصورة $6m + 1$.

"ملاحظة: أفرض وجود عد منتهي $p_1, \cdots, p_r$ ثم ضع $n = (2p_1 \cdots p_r)^2 + 3$"

(١١) (أ) برهن على وجود عدد غير منتهي من الأعداد الأولية التي على الشكل $8m - 1$.

"ملاحظة: أفرض وجود عدد منتهي $p_1, \cdots, p_r$ وضع $n = \prod_{i=1}^{r} p_i^2 - 2$"

(ب) برهن على وجود عدد غير منتهي من الأعداد الأولية التي على الشكل $8m+3$.

"ملاحظة: أفرض وجود عدد منتهي منها $p_1,\cdots,p_r$ وضع $n=\prod_{i=1}^{r}p_i^2+2$

(١٢) إذا كان $F_n=2^{2^n}+1$ عدداً أولياً ، فأثبت أن 3 جذر بدائي إلى F_n .

"ملاحظة: طبق مبرهنة (٦-٣-٦) " .

(١٣) أحسب (a/n) عندما $a=-1,-2,2,3,15,42$ ،

$$n=7,11,13,91,215$$

(١٤) (أ) إذا كان aRn ، فأثبت أن $(a/n)=1$.

(ب) بين بمثال على أنه إذا كان $(a/n)=1$ ، فإن aN_n.

****

الفصل السابع

بعض المعادلات الديوفنتية
Some Diophantine Equations

المعادلات الديوفنتية أو السيالة هي معادلات يقل عددها عن عدد المجاهيل الواردة فيها ، وبالتالي قد يكون لها عدد كبير من الحلول الممكنة (وهي حلول عددية صحيحة) .

هذا ولم يكن ديوفنتس الأسكندري "بين القرن الثالث والرابع للميلاد " أول من تعامل مع أمثال تلك المسائل (بل كان أول من بحثها بالتفصيل في كتابه المسائل العددية Arithmatica) لأن الفيثاغوريون حلوا المسألة $2x^2 - y^2 = 1$ قبل ديوفنتس بأكثر من قرنين ، وحلّ هيرون الأسكندري الذي عاش بين ١٥٠ق.م و ٢٥٠ للميلاد ، الكثير من المسائل السيالة مثل : إيجاد مستطيلين محيط الأول يساوي ثلاثة أمثال محيط الثاني ومساحة الأول تساوي مساحة الثاني .

أي $x + y = 3(z + w)$ ، $xy = zw$

وتعامل الهنود والصينيون مع أمثال تلك المعادلات ، ويعتقد بأن الهندي أريابهاتا (٤٧٦ ق.م) هو أول من وضع حلاً عاماً للمعادلات الديوفنتية بمجهولين .

وتعامل العرب والمسلمون مع المعادلات الديوفنتية ، فقد تطرق الخوارزمي (٧٨٠-٨٥٠م) في الجزء الأخير من كتابة "الجبر والمقابلة" وهو الجزء المخصص لمسائل التركة والقسمة إلى بعض المسائل غير المحدودة إلا أن لا شيء يدل على أهتمامه بالمعادلات الديوفنتية ، أما أبو كامل شجاع بن أسلم المصري (٨٥٠م – ٩٣٠م) فقد بيّن في كتابة "الطريف في الحساب" أن بعض المسائل تبقى وحيدة الحل وبعضها له عدة حلول بإعداد صحيحة وهي المسائل السيالة أو الديوفنتية ، وبعضها له عدة حلول بإعداد ليست صحيحة ، وقد أورد العديد من الأمثلة وحلها بطريقة تختلف عن الأسلوب الهندي .

أما في كتابة " كتاب في الجبر والمقابلة " الذي كتبه عام ٨٨٠م ، فقد عالج ثمانيـــة وثلاثون مسألة ديوفنتية من الدرجة الثانية ، وأربعة أنظمة معـــالات خطيـــة غيـــر محددة ، ومجموعة من مسائل تعود إلى متواليات حسابية.

وتناول الكرخي (ت ١٠٢٠م) في كتابة "البديع في الحساب" نظام خطـــي يحتـــوي على خمسة مجاهيل وهو

$$x+\frac{1}{3}(y+z+u)=s \quad ، \quad y+\frac{1}{4}(x+z+u)=s$$

$$z+\frac{1}{5}(x+y+u)=s \quad ، \quad u+\frac{1}{6}(x+y+z)=s$$

ومعادلات من النوع

$$ax^{2n}\mp bx^{2n-1}=y^2 \ , \ ax^{2n}\mp bx^{2n-2}=y^2$$

$$ax^2\mp bx+c=y^2 \quad , \ ax^2+c=y^2 \ , \ ax^2-c=y^2$$

ثم درس أنظمة المعادلات من الشكل $x^2-b=z^2 \ , \ x^2+a=y^2$

ودرس السموال المغربي (ت ٥٧٠ هـ) في كتابة "الباهر في الجبر" معادلات مـــن الشكل $y^3=ax+b$ ، $y^3=ax^2+bx$

هذا وتعامل المسلمون مـــع المعادلـــة $x^2+y^2=z^2$ وثلاثيـــات فيثـــاغورس أو المثلثات العددية القائمة الزاوية ، فقد أشار السموال المغربي في كتابة " الباهر فـــي الجبر" إلى أبحاث أبو سعيد السجزي (٩٥٠-١٠٢٤م) وابن الهيثم (٩٦٠-١٠٣٩م) في هذا المجال ، إضافة إلى حل السجزي للمعادلة $x^2=x_1^2+x_2^2+\cdots+x_n^n$. ويوجد بحثان آخران يعالجان المثلثات العددية القائمة الزاوية الأول لأبـــي جعفـــر الخازن (من علماء القرن الرابع الهجـــري) والآخـــر لأبـــي الجـــود بـــن الليـــث (ت ١٠٠٩م) . فقد أثبت الخازن أنه .

إذا كانت $x,y,z\in Z$ ، $(x,y)=1$ ، وكان x عدداً زوجياً ، فإن الشروط الآتيـــة متكافئة .

(١) $x^2 + y^2 = z^2$.

(٢) توجد أعداد صحيحة موجبة m,n ، $(m,n)=1$ وأحدهما فـردي والآخـر زوجي بحيث أن $x = 2mn \ , y = m^2 - n^2 \ , z = m^2 + n^2$.

ثم يثبت قضايا أخرى ، ويحل المعادلة $x^2 = x_1^2 + \cdots + x_n^2$. ويدرس المعادلتين $x^2 + y^2 = z^4$ ، $x^4 + y^2 = z^2$.

أما أبو الجود بن الليث فقد تطرق في رسالته عـن المثلثـات العدديـة القائمـة الزاوية، إلى مسألة تكونّ تلك المثلثات والشروط اللازمة لتكون المثلثـات البدائيـة "الثلاثيات البدائية" وينشئ جداول لتسجيل أضلاع المثلثـات الناتجـة ومـساحاتها ، ونسبة هذه المساحات إلى المحيطات ، وذلك انطلاقاً من ثنائيات أعداد صحيحة

$$(p,p+k) \text{ ، } k = 1,2,3,\cdots$$

أما محمد باقر اليزدي (ت ١٦٣٧م) فقد كتب بحثاً صغيراً لحل المعادلة الديوفنتية

$$x^2 = x_1^2 + x_2^2 + \cdots + x_n^2$$

أما مسألة تحليل عدد طبيعي إلى مجموع مربعات أعداد طبيعية فقد طرحت من قبل ديوفنش ، وبحثت في القرن العاشر للميلاد من قبل الخازن ، ونعلـم اليـوم إن هذه المسألة قادت باشيه (١٥٨١-١٦٣٨م) . ثـم فيرمـا (١٦٠١-١٦٦٥م) إلـى دراسة تمثيل عدد طبيعي (الأعداد الأولية تحديداً) على شكل مجموع مربعات .

أما المعادلتين $x^3 + y^3 = z^3$ ، $x^4 + y^4 = z^4$ ، فقد بحثت من قبـل كـل مـن الكرخي والخجندي (ت ١٠٠٠م) والخازن وابـن سـينا (٩٨٠-١٠٣٨) والخيـام (١٠٤٨-١١٣١) والبيرونـــي (٩٧٣-١٠٥٠م) ، وابـــن الخـــوام البغـــدادي (١٢٤٥-١٣٢٤م) وكمال الدين الفارسي (ت ١٣٢٠م) مؤكدين عدم وجود أعـداد صحيحة تحقق أياً منهما . أما المعادلة $x^n + y^n = z^n$ ، $n \geq 3$ فقد درست مـن قبل فيرما مؤكداً عدم وجود أعـداد صـحيحة تحقـق تلـك المعادلـة بـشرط أن $xyz \neq 0$ ، وقد أثبت الإنجليزي أندرو وايلس صحة ذلك سنة ١٩٩٤م ومنح عليه ميدالية فيلد في الرياضيات .

هذا وتوجد معادلات ديوفنتية مهمة أخرى مثل المعادلة $x^2 - dy^2 = 1$، حيث d ليست مربعاً كاملاً والتي تنسب إلى الإنجليزي جون بل (١٦١١-١٦٨٥م) بدلاً من فيرماً الذي وضعها سنة ١٦٥٧م مخمناً وجود حل واحد على الأقل لتلك المعادلة يختلف عن $x = \mp 1$ ، $y = 0$. فمثلاً أقل قيم إلى x, y تحقق المعادلة $x^2 - 5y^2 = 1$ هي $x = \pm 9$ ، $y = \mp 4$. أما أقل قيم إلى x, y تحقق المعادلة $x^2 - 43y^2 = 1$ فهي $x = \mp 3482 , y = \mp 531$.

وقد أُثْبِتَ تخمين فيرما من قبل الفرنسي لاجرانج (١٧٣٩-١٨١٣م) سنة ١٧٦٨م ونشر الألماني ديركلي (١٨٠٥-١٨٥٩م) سنة ١٨٣٧ طريقة لحساب أقل الأعداد التي تحقق المعادلة $x^2 - dy^2 = 1$ استخدم فيها الدوال المثلثية ، وأعطى الألماني كرونكر (١٨٢٣-١٨٩١) سنة ١٨٦٣م طريقة أخرى لحساب أقل الأعداد التي تحقق تلك المعادلة بإستخدام الدوال الناقصية (Elliptic function) .

أما المعادلة الديوفنتية $x^p - y^q = 1$ التي وضعها كاتلان سنة ١٨٤٤م وخمّن بأنه إذا كان $x, y \in Z$ ، p, q ، فإن الحل الوحيد لهذه المعادلة هو $p = y = 2 , q = x = 3$. وقد أثبت ميهيلسكو (Mihailescu) سنة ٢٠٠٣م صحة ذلك التخمين .

أما المعادلة الديوفنتية $n!+1 = x^2$ ، فيعود تاريخها إلى سنة ١٨٨٥م عندما خمّن بروجارد (Brochard) بأن الحلول الوحيدة لها في Z هي $4!+1 = 5^2 , 5!+1 = 11^2 , 71+1 = (71)^2$ ، وفي سنة ١٨٩٥م كتب الهندي رامنجين (١٨٨٧-١٩٢٠) نفس التخمين ، وقد أثبت كرايجك (Kraitichik) صحة ذلك التخمين لكل $n \leq 5000$.

أما المعادلة الديوفنتية $y^2 = x^3 + k$ والتي تسمى معادلة موردل (Mordell Equation) المكتشفة سنة ١٩٢٢م من قبل الإنجليزي موردل (١٨٨٨-١٩٧٢) والتي تمثل منحياً ناقصاً (Elliptic curve) في المستوى

الأسقاطي الحقيقي(Real projective plane) ، فإن وجود أو عدم وجـود أعـداد صحيحة تحقق المعادلة يعتمد على قيمة k . فإذا كان $k=1$ ، فإن الحلول الوحيدة في Z للمعادلة $y^2=x^3+1$ هي $(2,\mp 3)$, $(-1,0)$, $(0,\mp 1)$. أما إذا كـان $k=-5$ ، فليس للمعادلة $y^2=x^5-5$ حل في Z ، وإذا كان $k=-28$ ، فإن الحلول الوحيدة في Z لتلك المعادلة هي $(37,\mp 225)$, $(8,\mp 22)$, $(4,\mp 6)$.

٧-١: المعادلات الديوفنتية الخطية Linear Diophantine Equations

يعتبر هذا النوع من أبسط أنواع المعادلات الديوفنتية ، وسنركز أهتمامنا فـي هذا الجزء على حل المعادلتين :

$$ax+by=c \quad ، \quad ax+by+cz=e$$

ونبدأ بما يلي :

مبرهنة ٧-١-١:

(أ) يوجد حل للمعادلـة $ax+by=c$ ، إذاً وإذا فقـط كـان $d\backslash c$ ، حيـث $d=(a,b)$.

(ب) إذا كان x_1 , y_1 حلاً للمعادلة $ax+by=c$ ، فـإن أي حـل آخـر لهـذه المعادلة يكون على الشكل :

$x=x_1+(b/d)t \ , \ y=y_1-(a/d)t$ ، حيث $t\in Z$.

البرهان:

(أ) نفرض أن x_1 ,y_1 حـل للمعادلـة $ax+by=c$. إذاً $ax_1+by_1=c$. لكن $d=(a,b)$. إذاً $d\backslash a$ و $d\backslash b$ ، وعليه فإن $d\backslash(ax_1+by_1)$ حسب مبرهنة (٢-١-١هـ) ، وبالتالي فإن $d\backslash c$.

ولإثبات العكس نفرض أن $d\backslash c$. إذاً يوجد $r\in Z$ ، بحيـث أن $c=dr$.

لكن $d=(a,b)$. إذاً يوجد $m,n\in Z$ بحيث $d=am+bn$ حسب مبرهنة (٢-١-٥أ) . إذاً $c=rd=arn+brm$ ، وعليه فإن $x=rm$ ، $y=rn$ حل للمعادلة $ax+by=c$.

(ب) بما أن x_1,y_1 حل للمعادلة $ax+by=c$. إذاً $ax_1+by_1=c$. والآن فنفرض أن u,w حل آخر للمعادلة $ax+by=c$. إذاً $au+bw=1$ ، وعليه فإن

$$ax_1+by_1=au+bw \Leftrightarrow a(u-x_1)=b(y_1-w) \qquad \dots (1)$$

لكن $d=(a,b)$. إذاً يوجد $r,s\in Z$ ، بحيث أن $(r,s)=1$ و

$$a=dr \ , \ b=ds \qquad \dots (2)$$ حسب نتيجة (١) مبرهنة (٢-١-٨)

ومن (1) ، (2) ينتج أن

$$r(u-x_1)=s(y_1-w) \qquad \dots (3)$$

وعليه فإن $s\backslash r(u-x_1)$ ، لكن $(r,s)=1$. إذاً $s\backslash(u-x_1)$ حسب مبرهنة (٢-٢-٣أ) ، وعليه فإن

$$u-x_1=st \ ، \ t\in Z \ ، \text{إذاً} \ u=x_1+st=x_1+(b/d)t \qquad \dots (4)$$

ومن (3) ، (4) ينتج أن $y_1-w=rt$ ، وعليه فإن $w=y_1-rt=y_1-(a/d)t$. لكن

$$ax+by=a[x_1+(b/d)t]+b[y_1-(a/d)t]=ax_1+by_1=c$$

وعليه فإن $x=x_1+(b/d)t$ ، $y=y_1-(a/d)t$ حل للمعادلة $ax+by=c$

□

<u>نتيجة :</u>

إذا كان $(a,b)=1$ ، وكان x_1,y_1 حلاً للمعادلة $ax+by=c$ ، فإن أي حل آخر لهذه المعادلة يكون على الصورة $x=x_1+bt$ ، $y=y_1-at$ ، $t\in Z$ يسمى x_1,y_1 الحل الخاص (Particular solution) للمعادلة $ax+by=c$.

مثال (١) :

حل المعادلة

$$24x + 68y = 36 \qquad \dots (5)$$

الحل :

بما أن $d = (24,68) = 4$ و $4 \setminus 36$. إذاً يوجد حل للمعادلة (5) حسب مبرهنة (٧-١-١) ، ولإيجاد الحل . لاحظ أنه بإستخدام القسمة الخوارزمية ، نجد أن $d = 4 = 3(24) + 68(-1)$ ، وعليه فإن

$$36 = 9d = 9 \cdot 3 \cdot 24 + 9 \cdot 68(-1) = 27 \cdot 24 + 68(-9)$$

وبالتالي فإن $x_1 = 27$ ، $y_1 = -9$ ، وعليه فإن $x = 27 + \frac{68}{4} \cdot t = 27 + 17t$ ، $y = -9 - \frac{24}{4} \cdot t = -9 - 6t$ ، $t \in Z$ حل للمعادلة (5) .

مثال (٢) :

حل المعادلة

$$5x + 13y = 28 \qquad \dots (6)$$

الحل :

بما أن $(5,13) = 1$. إذاً يوجد حل للمعادلة (6) حسب مبرهنة (٧-١-١) ولإيجاد ذلك الحل ، لاحظ أن $1 = 5(-5) + 13(2)$ ، إذاً

$28 = 28(5)(-5) + 28(13)(2) = 5(-140) + 13(56)$ ، وعليه فإن $x_1 = -140 , y_1 = 56$ حل خاص للمعادلة (6) . أما الحل العام هو

$$y = y_1 - at = 56 - 5t \quad , \quad x = x_1 + bt = -140 + 13t \text{ حيث } t \in Z$$

ملاحظة :

قد يكون من المفيد إيجاد الحلول الموجبة للمعادلة $ax + by = c$.

ولإيجادها يجب أن يكون $x = x_1 + (b/d)t > 0 \,,\; y = y_1 - (a/d)t > 0$.

مثال (٣) :

أوجد الحلول الموجبة للمعادلة

$$499x - 49y = 300 \qquad \dots (7)$$

الحل :

بما أن $(499,-49) = 1$. إذاً يوجد حل للمعادلة (7) حسب مبرهنة (٧-١-١) ولإيجاد ذلك الحل ، لاحظ أن

$$499x - 49y = 300 \Rightarrow 499x \equiv 300 (\bmod 49) \wedge -49y \equiv 300 (\bmod 499)$$

وبحل التطابق $499x \equiv 300 (\bmod 49)$ ، نجد أن $9x \equiv 6 (\bmod 49)$ ، وعليه فإن $3x \equiv 2 (\bmod 49)$ وبالتالي فإن $49z \equiv -2 (\bmod 3)$ حسب الملاحظة ص (٩٦) ، ومنها نجد أن $z \equiv -2 \equiv 1 (\bmod 3)$ ، وعليه فإن $z = 1 + 3t$ ، $t \in Z$. لكن $x = \frac{nz + b}{a}$. إذاً

$$x = \frac{49(1+3t)+2}{3} = 17 + 49t \text{ ، } y = \frac{499(17+49t)-300}{49} = 167 + 499t$$

ومن الواضح أن $x > 0$ ، $y > 0$ لكل $t \in Z^+$ ، وعليه يوجد عدد غير منتهي من الحلول الموجبة إلى المعادلة (7) .

مثال (٤) :

حدد الحلول الموجبة (أن وجدت) للمعادلة

$$472x + 531y = 1121 \qquad \dots (8)$$

الحل :

بما أن $(472,531) = 59$ و $59 \backslash 1121$. إذاً للمعادلة (8) حل حسب مبرهنة (٧-١-١) . ولإيجاد هذا الحل ، لاحظ أن

$$59 = 472(-1) + 531$$

إذاً $1121 = 19(59) = 472(-19) + 531(19)$ ، وعليه فإن $x_1 = -19, y_1 = 19$.

أما الحل العام فهو

$$x = x_1 + (b/d)t = -19 + \frac{531}{59}t = -19 + 9t$$

$$y = y_1 - (a/d)t = 19 - \frac{472}{59}t = 19 - 8t$$ لكل $t \in Z$

لكن $x > 0$ و $y > 0$ يعني أن $t > \frac{19}{9}$ و $t < \frac{19}{8}$. وعليه فإن $\frac{19}{9} < t < \frac{19}{8}$

ولكن لا يوجد عدد صحيح بين $\frac{19}{9}, \frac{19}{8}$. إذاً لا يوجد حل صحيح موجب للمعادلة (8) .

<u>مثال (٥) :</u>

أوجد الحلول الموجبة للمعادلة

$$44x + 20y = 600 \qquad \ldots (9)$$

<u>الحل :</u>

بما أن $d = (44,20) = 4$ و $4 = 44 + 20(2)$. إذاً

$$600 = 150(4) = 44(150) + 20(-300)$$

وعليه فإن $x_1 = 150 \;,\; y_1 = -300$ ويكون الحل العام هو

$$x = 150 + 5t \;,\; y = -300 - 11t \;,\; t \in Z$$

لكن $x > 0$ يعني أن $t > -30$، أما $y > 0$ فيعني أن $t < \frac{-300}{11} = -27.27$

إذاً $-30 < t < -27.27$ و $t \in Z$، يعني أن $t = -29 , -28$ ، وعليه فإن الحلول الموجبة للمعادلة (9) هي

$$x = 150 - 145 = 5 \quad , \quad y = -300 + 319 = 19$$

$$x = 150 - 140 = 10 \quad , \quad y = -300 + 308 = 8$$

والآن إلى المثال الآتي . الذي ورد في كتاب "الطريف في الحساب" لأبي كامل شجاع بن أسلم المصري (٨٥٠-٩٣٠م) ، والذي يختزل فيه نظاماً من معادلتين ديوفنتين إلى معادلة واحدة بمتغيرين ويحلها .

مثال (٦) :

دُفع إليك مائة درهم ، فقيل لك ابتع مائة طائر من حمام وبط ودجاج . فإذا كانت البطة بدرهمين ، والحمام كل ثلاثة بدرهم ، والدجاج كل أثنين بدرهم . فكم تشتري من كل نوع .

الحل :

نفرض أن عدد الحمام = x ، عدد الدجاج = y ، عدد البط = z . إذاً

$$x + y + z = 100 \quad \dots (1)$$ ،

$$\frac{x}{3} + \frac{y}{z} + 2z = 100 \quad \dots (2)$$

ومن (1) نجد أن $z = 100 - (x + y)$ ، وبالتعويض في (2) ينتج أن

$$10x + 9y = 600 \quad \dots (3)$$

لكن $(10,9) = 1$ ، $1 = 10 - 9$ ، إذاً $600 = 10(600) + 9(-600)$ ، وعليه فإن $x_1 = 600 \ , \ y_1 = -600 \ , \ z_1 = 100$ ، وبالتالي فإن

$$x = x_1 + bt = 600 + 9t \quad , \ y = y_1 - at = -600 - 10t$$

$$z = 100 - (600 + 9t - 600 - 10t) = 100 + t > 0 \qquad \forall t \in N$$

$$x > 0 \Rightarrow t > -\frac{200}{3} = -66.66 \ , \ y > 0 \Rightarrow t < -60$$

إذاً $-66.66 < t < -60$ ، وعليه فإن

$t = -66 \ , -65 \ , 64 , -63 , -62 , -61$

$x = 6 \quad , \quad y = 60 \quad , \quad z = 40$

$x = 15 \quad , \quad y = 50 \quad , \quad z = 35$

$x = 24 \quad , \quad y = 40 \quad , \quad z = 36$

$x = 33 \quad , \quad y = 30 \quad , \quad z = 37$

$x = 42 \quad , \quad y = 20 \quad , \quad z = 38$

$x = 51 \quad , \quad y = 10 \quad , \quad z = 39$

وهذا ما وجده ابن أسلم المصري .

والآن إلى المبرهنة الآتية التي تضمن وجود حل للمعادلة الديوفنتية بأكثر من مجهولين .

مبرهنة ٧-١-٢ :

يوجد حل للمعادلة الديوفنتية

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = c \quad ، \quad n \geq 2 \; . \qquad \dots (10)$$

إذاً وإذا فقط كان $(a_1, a_2, \cdots, a_n) \setminus c$

البرهان :

ليكن $d = (a_1, a_2, \cdots, a_n)$ ، وليكن $y_1, \dots, y_n$ حلاً للمعادلة (10) . إذاً $\sum_{i=1}^{n} a_i y_i = c$. لكن $d \setminus a_i$ لكل $i = 1, \dots, n$. إذاً $d \setminus (\sum_{i=1}^{n} a_i y_i)$. وعليه فإن $d \setminus c$.

ولإثبات العكس نفرض أن $d \setminus c$. إذاً يوجد $r \in Z$ بحيث أن $c = dr$. لكن $d = (a_1, \dots, a_n)$. إذاً يوجد $y_1, \dots, y_n \in Z$ بحيث أن $\sum_{i=1}^{n} a_i y_i = d$ حسب مبرهنة (٢-١-٧) ، وعليه فإن $\sum_{i=1}^{n} a_i (r y_i) = rd = c$ ، وبالتالي فإن $x_1 = r y_1 , x_2 = r y_2 , \dots , x = r y_n$ حل للمعادلة (10) .

□

ملاحظة :

لإيجاد الحل العام للمعادلة الديوفنتية التي تحتوي على أكثر من مجهولين ، نختزل تلك المعادلة إلى معادلة بمجهولين ، ثم نوجد الحل ، وتوجد طريقتان لحل مثل تلك المعادلات .

الطريقة الأولي : ليكن

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = c \quad ، \quad n > 2 \; . \qquad \dots (10)$$

وليكن $d = (a_1, \cdots, a_n)$ ، $d \setminus c$ ، ولنفرض أن

$$x_{n-1} = \alpha u + \beta v \quad , \quad x_n = \gamma u + \delta v \qquad \dots (11)$$

نختار $\alpha,\beta,\gamma,\delta$ بحيث أن $\alpha\delta-\beta\gamma=1$ ، وعليه فإن

$$v=-\gamma x_{n-1}+\alpha x_n \quad , \quad u=\delta x_{n-1}-\beta x_n$$

إذاً $u,v,\in Z \Leftrightarrow x_{n-1} , x_n \in Z$.

وإذا كان $\delta=\dfrac{-a_{n-1}}{(a_{n-1},a_n)}$ ، $\beta=\dfrac{a_n}{(a_{n-1},a_n)}$ ، فإن $(\beta,\delta)=1$.

وبالتالي يمكن حل المعادلة $\alpha\delta-\beta\gamma=1$ وإيجاد α,γ، وبالتعويض في (10) نجد أن

$$ax_1+a_2x_2+...+a_{n-2}x_{n-2}+(a_{n-1}\alpha+a_n\gamma)u=c \qquad ... (12)$$

وعدد المتغيرات في (12) أقل بواحد من عدد المتغيرات في (10) . ونلاحظ أن

$$a_{n-1}\alpha+a_n\gamma=-(a_{n-1},a_n)\alpha\delta+(a_{n-1},a_n)\beta\gamma=-(a_{n-1},a_n)$$

$$d=(a_1,a_2,...,a_{n-2},(a_{n-1},a_n))=(a_1,a_2,...,a_n)$$

إذاً للمعادلة (12) نفس خواص المعادلة (10) وهذا يعني أن c يقبل القسمة على القاسم المشترك الأعظم لمعاملاتها ، كما أن معامل من تلك المعاملات لا يساوي صفراً .

وإذا كان $n>3$ ، فيمكن تطبيق ما سبق على المعادلة (12) والحصول على معادلة عدد متغيراتها $(n-2)$. إذاً بإعادة الطريقة أعلاه عدة مرات نحصل على معادلة بمتغيرين يمكن إيجاد الحل العام لها ، وتوضح الأمثلة الآتية هذه الطريقة .

<u>**مثال (٧) :**</u>

حل المعادلة

$$15x+10y+6z=61 \qquad ... (13)$$

<u>**الحل :**</u>

بما أن $(15,10,6)=1$. إذاً يوجد حل للمعادلة (13) حسب مبرهنة (٧-١-٢)، ولإيجاد ذلك الحل نفرض أن

$\alpha\delta-\beta\gamma=1$, $z=\gamma u+\delta v$, $y=\alpha u+\beta v$. إذاً

$10y+6z=(10\alpha+6\gamma)u+(10\beta+6\delta)v$ ولحذف v ضع $\beta=3\ ,\ \delta=-5$ تجد أن $\alpha\delta-\beta\gamma=1\Rightarrow -5\alpha-3\gamma=1$ ، وعليه إذا كان $\alpha=1$ ، فإن $\gamma=-2$ ، وبالتالي فإن

$$y=u+3v \quad , \quad z=-2u-5v \qquad \ldots(14)$$

ومن (13) ، (14) نجد أن الحل العام للمعادلة (13) هو

$$x=2t+1 \qquad , \qquad u=15t-23$$

$$y=15t+3v-23 \qquad , \qquad z=-30t-5v+46$$

حيث $t,v\in Z$

وعندما $t=v=1$ ، نجد أن $z=11\ ,\ y=-5\ ,\ x=3$ حل للمعادلة (13)

وعندما $t=2,v=1$ ، نجد أن $z=-19\ ,\ y=10\ ,\ x=5$ حل للمعادلة (13)

وعندما $t=2,v=-1$ ، نجد أن $z=-9\ ,\ y=4\ ,\ x=5$ حل للمعادلة (13)

مثال (٨) :

حل المعادلة

$$3x-6y+5z=11 \qquad \ldots(15)$$

الحل :

بما أن $(3,-6,5)=1$. إذاً يوجد حل للمعادلة (15) حسب مبرهنة (٧-١-٢)، ولإيجاد ذلك الحل ، نفرض أن

$$y=\alpha u+\beta v \quad , \quad z=\gamma u+\delta v\ ,\ \alpha\delta-\beta\gamma=1$$

إذاً $-6y+5z=(-6\alpha+5\gamma)u+(-6\beta+5\delta)v=0$ ، ولحذف v ، ضع $\beta=5\ ,\ \delta=6$، تجد أن

$$6\alpha-5\gamma=1\Rightarrow \alpha=\gamma=1 \qquad \ldots(16)$$

ومن (15) ، (16) ينتج أن

$$3x-u=11 \qquad \ldots(17)$$

وعليه فإن $u \equiv -11 \equiv 1 (\mod 3)$ ، وبالتالي فـإن $u = 1 + 3t$ ، وبـالتعويض في (17) ينتج أن $x = 4 + t$ ، $t \in Z$. إذاً

$$z = \gamma u + \delta v = 1 + 3t + 6v \text{ و } y = \alpha u + \beta v = 1 + t + 5v \text{ ، } v \in Z$$

وعندما $t = v = 0$ ، نجـد أن $z = 1 \ , \ y = 1 \ , \ x = 4$ حـل للمعادلـة (15)

وعندما $t = v = 1$ ، نجـد أن $z = 10 \ , \ y = 9 \ , \ x = 5$ حـل للمعادلـة (15)

وعندما $t = 1, v = 2$ ، نجد أن $z = 16 \ , \ y = 14 \ , \ x = 5$ حل للمعادلة (15)

الطريقة الثانية: "طريقة اويلر"

وتعتمد هذه الطريقة على كون مجموع أو الفرق بين عددين صـحيحين يكـون عدداً صحيحاً ، ونوضح هذه الطريقة بمثالين أحدهما سبق حله بالطريقة السابقة .

مثال (٩) :

حل المعادلة

$$5x + 10y + 6z = 61 \qquad \dots (18)$$

الحل :

نختار المجهول الذي قيمه معامله المطلقة هي الصغرى فنجد أنـه 6 ثـم نقسم طرفي المعادلة على ذلك المعامل، فنجد أن

$$\frac{5}{2}x + \frac{5}{3}y + z = \frac{61}{6}$$

ومنها نجد أن

$$z = \frac{61}{6} - \frac{5}{2}x - \frac{5}{3}y = 10 + \frac{1}{6} - 2x - \frac{1}{2}x - y\frac{2}{3}y \qquad \dots (19)$$

نأخذ الجزء الكسري ونفرض أنه t_1 ، إذاً

$$t_1 = \frac{1}{6} - \frac{1}{2}x - \frac{2}{3}y \qquad \dots (20)$$

ومنها نجد أن $6t_1 = 1 - 3x - 4y$ ، وعليه فإن

$$y = \frac{1}{4} - \frac{3}{4}x - \frac{3}{2}t_1 = \frac{1}{4} - \frac{3}{4}x - t_1 - \frac{1}{2}t_1 \qquad \dots (21)$$

نأخذ الجزء الكسري ونفرضه t_2 ، إذاً $t_2 = \frac{1}{4} - \frac{3}{4}x - \frac{1}{2}t_1$ ، وعليه فإن

$4t_2 = 1 - 3x - 2t_1$ ، ومنها نجد أن

$$x = \frac{1}{3} - \frac{2}{3}t_1 - \frac{4}{3}t_2 = \frac{1}{3} - \frac{2}{3}t_1 - t_2 - \frac{1}{3}t_2 \qquad \dots (22)$$

وعليه فإن $t_3 = \frac{1}{3} - \frac{2}{3}t_1 - \frac{1}{3}t_2$ ، ومنها نجد أن $3t_3 = 1 - 2t_1 - t_2$

وعليه فإن

$$t_2 = 1 - 2t_1 - 3t_3 \qquad \dots (23)$$

ونتوقف هناك لأن معامل أحد المتغيرات أصبح واحد وهو معامل t_2

ومن (22) ، (23) نجد أن

$$x = 2t_1 + 4t_3 - 1 \quad ، \quad t_1, t_3 \in Z \qquad \dots (24)$$

ومن (21) ، (24) ، نجد أن

$$y = 1 - 3t_1 - 3t_3 \qquad \dots (25)$$

ومن (24) ، (25) ، (19) ينتج أن

$$z = 11 - 5t_3$$

وعندما $t_3 = 0 \ , \ t_1 = 2$ ، نجد أن

$$x = 3 \ , \ y = -5 \ , \ z = 11$$

وعندما $t_3 = 6 \ , \ t_1 = -9$ ، نجد أن

$$x = 5 \ , \ y = 10 \ , \ z = 19$$

وعندما $t_3 = 4 \ , \ t_1 = -5$ ، نجد أن

$$x = 5 \ , \ y = 4 \ , \ z = -90$$

وهي نفس الحلول التي حصلنا عليها سابقاً .

مثال (١):

حل المعادلة

$$15x + 12y + 30z = 24 \qquad \dots (26)$$

الحل :

بما أن $3 = (15,12,30)$ و $3 \backslash 24$. إذاً يوجد حل للمعادلة (26) حسب مبرهنة (٧-١-٢) . ولإيجاد ذلك الحل نقسّم طرفي المعادلة على معامل y ، فنجد أن

$\frac{5}{4}x + y + \frac{5}{2}z = 2$ ، ومنها نجد أن ... (27)

$y = 2 - \frac{5}{4}x - \frac{5}{2}z = 2 - x - \frac{1}{4}x - 2z - \frac{1}{2}z$ ، وعليه فإن ... (28)

$t_1 = -\frac{1}{4}x - \frac{1}{2}z$ ، وعليه فإن $4t_1 = -x - 2z$ وبالتالي فإن ... (29)

$x + 2z + 4t_1 = 5$ ونتوقف هنا لأن أصغر معامل هو واحد ، وعليه فإن

$x = -2z - 4t_1$ ... (30)

ومن (28) ، (30) ينتج أن $y = 2 + 5t_1$ ، وبوضع $z = t_2$ يكون الحل العام هو

$z = t_2 \ , \ y = 2 + 5t_1 \ , \ x = -2t_2 - 4t_1$ ، حيث $t_1, t_2 \in Z$.

وعندما $t_1 = t_2 = 1$ ، نجد أن

$z = 1 \ , \ y = 7 \ , \ x = -6$ حل للمعادلة (26)

وعندما $t_1 = -1 \ , \ t_2 = 1$ ، نجد أن

$z = 1 \ , \ y = -3 \ , \ x = 2$ حل للمعادلة (26)

تمـــارين

(١) أوجد جميع الحلول لكل من المعادلات الديوفنتية الآتية:

(أ) $14x + 18y = 10$ ، (ب) $24x + 112y = 32$

(ج) $156x + 91y = 130$ ، (د) $3x + 5y = 19$

(هـ) $20x + 51y = 353$ ، (و) $701x - 137y = 1434$

(٢) أوجد جميع الحلول الموجبة لكل مما يأتي:

(أ) $15x + 17y = 113$ ، (ب) $23x + 57y = 765$

(ج) $3x + 5Y = 17$ ، (د) $79x + 77y = 1446$

(٣) حل كلاً من المعادلات الديوفنتية الآتية:

(أ) $x + 3y + 2z = 1$ ، (ب) $3x - 2y - 6z = 1$

(ج) $5x + 4y + 3z = 22$ ، (د) $3x + 14y - 38z = 58$

(هـ) $x - 2y + 3z = 50$ ، (و) $5x + 8y - 3z = 10$

(٤) إذا كان $(a,b) = 1$ فبرهن على وجود عدد غير منتهي من الحلول للمعادلة $ax - by = 1$.

(٥) أثبت أن $ax + by = a + c$ قابلة للحل إذاً وإذا فقط كان $ax + by = c$ قابلة للحل .

(٦) أثبت أن $ax + by = c$ قابلة للحل إذاً وإذا فقط كان $(a,b) = (a,b,c)$.

(٧) "ابن أسلم المصري"

دفع إليك مائة درهم فقيل لك ابتع مائة طائر من البط والحمام والقنابر والدجاج. كل بطه بدرهمين ، والحمام اثنان بدرهم والقنابر ثلاثة بدرهم والدجاج كل واحدة بدرهم. فكم تشتري من كل نوع.

(٨) دُفع البنك مائة ريال ، فقيل أشتري ثلاث أصناف من الفواكه برتقال ، وتفاح وكمثرى . فإذا كان كل ستة تفاحات بخمسة ريالات وكل خمسة تفاحات بأربعة ريالات والكمثرى كل ثلاثة بريالين فما عدد ما تشتري من كل نوع .

٧-٢ : المعادلة $x^2 + y^2 = z^2$ وثلاثيات فيثاغورس .

يعرف البابليون والمصريون بأن المثلث الذي أطوال إضلاعه 3,4,5 قائم الزاوية بل يعرف البابليون أن كل مثلث من المثلثات الذي أطوال إضلاعه

(45,60,75) , (65,72,97) , (119,120,169) , (319,360,481)
(1679,2400,2929) , (1771,2700,3229) , (4601,4800,6649)
(4961,6480,8161) , (12709,13500,18541)

قائم الزاوية ، واستنتجوا من ذلك المبرهنة الآتية: **مجموع المربعين المنشأين على الضلعين القائمين في المثلث القائم الزاوية يساوي المربع المنشأ على الوتر .**

أي إذا كان x,y طولي ضلعي الزاوية القائمة وكان z طول الوتر فإن

$$x^2 + y^2 = z^2 \qquad \dots (1)$$

أما نسبة هذه المبرهنة إلى فيثاغورس (٥٨٤ - ٤٩٥ق.م) فيعتقد أنه أول من برهنها ، كما ينسب إلى فيثاغورس وإلى إقليدس وجود عدد لا نهائي من الأعداد التي على الصورة :

$x = 2n + 1 \ , \ y = 2n^2 + 2n \ , \ z = 2n^2 + 2n + 1$ تحقق المعادلة (1)

هذا ولقد ترجم وحلّل المؤرخ الألماني فرانز ويبكه (Franz woepche) (١٨٢٦-١٨٦٤) في القرن التاسع عشر [٤،٥] بحثين لرياضيين من القرن العاشر للميلاد ، يعالجان المثلثات العددية قائمة الزاوية (ثلاثيات فيثاغورس) . الأول لرياضي مجهول الأسم والثاني لأبي جعفر الخازن تؤكد بأنها جديدة ومجهولة من قبل الأقدمين والمعاصرين . إذا يقول كاتب النص مجهول المؤلف بعد أن يعطي مبدأ تكوين المثلثات العددية قائمة الزاوية " **هذا هو الأصل في معرفة الأقطار للمثلثات التي هي أصول الأجناس (الثلاثيات البدائية) ، ولم أجد هذا ذكر في شيء من الكتب القديمة ولا ذكره أحد ممن وضع الكتب في الحساب من المحدثين ولا علمت أنه أنفتح لأحد من قبلي** " .

أما الخازن فينص ويبرهن بعض المقدمات المتعلقة بخواص الثلاثيات البدائية ، ثم يثبت أن :

إذا كان x عدداً زوجياً وكان y عدداً فردياً و $x^2 + y^2 = z^2$ فيوجد $m,n \in N$ بحيث أن $m > n > 0$ و $z = m^2 + n^2$, $y = m^2 - n^2$, $x = 2mn$

ثم يوجد الحلول لكل من المعادلتين $x^2 + y^2 = z^4$ ، $x^4 + y^2 = z^2$.

تعريف ٧-٢-١ :

يقال عن ثلاثي من الأعداد الطبيعية x,y,z أنه ثلاثي فيثاغورس (Pythagorean Triple) ، إذا كان $x^2 + y^2 = z^2$.

ويقال عن ثلاثي فيثاغورس (x,y,z) ، أنه : ثلاثي بدائي (Primitive Triple) ، إذا كان $(x,y,z) = 1$.

مثال (١) :

(أ) كل من $(3,4,5)$ ، $(5,12,13)$ ، $(11,60,61)$ ثلاثي فيثاغورس بدائي.

(ب) كل من $(6,8,10)$ ، $(10,24,26)$ ، $(42,40,58)$ ثلاثي فيثاغورس.

ولكي نوجد جميع الثلاثيات الفيثاغورسية البدائية ، نورد الآتي .

مبرهنة ٧-٢-١ :

(x,y,z) ثلاثي فيثاغورس إذاً وإذا فقط وجد $d \in Z^+$ ، وثلاثي بدائي (a,b,c) بحيث أن $z = cd$, $y = bd$, $x = ad$.

البرهان :

نفرض أن (x,y,z) ثلاثي فيثاغورس ، وأن $d = (x,y,z)$. إذاً $d > 0$ و $(a = \frac{x}{d}, b = \frac{y}{d}, c = \frac{z}{a})$ ثلاثي فيثاغورس بدائي ، لأن

$$a^2 + b^2 = (\frac{x}{d})^2 + (\frac{y}{d})^2 = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = (\frac{z}{d})^2 = c^2$$ و $(a,b,c) = 1$

ولإثبات العكس نفرض أن (a,b,c) ثلاثي فيثاغورس بدائي ، $d \in Z^+$. إذاً $(x=ad \;,\; y=bd \;,\; z=cd)$ ثلاثي فيثاغورس ، لأن

$$x^2+y^2=(ad)^2+(bd)^2=(a^2+b^2)d^2=c^2d^2=z^2$$

□

مبرهنة ٧-٢-٢ :

إذا كان (x,y,z) ثلاثياً فيثاغورس بدائياً ، فإن $(x,y)=(x,z)=(y,z)=1$.

البرهان :

نفرض أن $(x,y)=d>1$. إذاً يوجد عدد أولي p ، بحيث أن $p \backslash x$ و $p \backslash y$ حسب مبرهنة (٢-٢-٤أ) ، وعليه فإن $p \backslash x^2$ و $p \backslash y^2$ ، وبالتالي فإن $p \backslash (x^2+y^2)$. لكن $x^2+y^2=z^2$ بالفرض ، إذاً $p \backslash z^2$ ، وعليه فإن $p \backslash z$ ، وبالتالي فإن $(x,y,z)=p>1$ وهذا يناقض كون (x,y,z) ثلاثياً فيثاغورسياً بدائياً . وبنفس الطريقة نبرهن أن $(x,z)=(y,z)=1$.

□

مبرهنة ٧-٢-٣ : " الخازن "

إذا كان (x,y,z) ثلاثياً فيثاغورس بدائياً ، فإما x زوجي و y فردي أو x فردي و y زوجي .

البرهان :

بما أن $(x,y,z)=1$. إذاً $(x,y)=1$ حسب مبرهنة (٧-٢-٢) ، وعليه لا يمكن أن يكون x,y زوجين معاً . وإذا كان كل من x,y عدداً فردياً ، فإن $x=2m+1 \;,\; y=2n+1$ ، حيث $m,n \in Z^+$ ، وعليه فإن

$$z^2=x^2+y^2=4m^2+4n^2 4m+4n+2 \equiv 2 (\mathrm{mod}\ 4)$$

وهذا غير ممكن .

□

والآن إلى مبرهنات الخازن الآتية التي توضح كيفية إيجاد ثلاثيات فيثاغورس البدائية .

مبرهنة ٧-٢-٤ :

إذا كان $a,b \in Z^+$ ، $(a,b)=1$ ، وكان ab مربعاً كاملاً ، فإن كلاً من a,b مربع كامل .

البرهان :

بما أن $a=\prod_{i=1}^{r} p_i^{e_i}$ ، $b=\prod_{j=1}^{s} q_j^{\alpha_j}$ ، حيث q_j , p_i أعداد أولية حسب المبرهنة الأساسية في الحساب ، وبما أن $(a,b)=1$. إذاً p_i , q_j أعداد أولية مختلفة لكل i,j. لكن $ab=\prod_{i=1}^{r} p_i^{e_i} \cdot \prod_{j=1}^{s} q_j^{e_j}$ مربع كامل بالفرض . إذاً كل من e_i , α_j عدد زوجي لكل i,j ، وعليه فإن كلاً من a,b مربع كامل .

□

مبرهنة ٧-٢-٥ : " الخازن "

إذا كان $x,y,z \in Z^+$ وكان x عدداً زوجياً ، فإن (x,y,z) ثلاثي فيثاغورس بدائي إذاً وإذا فقط كان وجد $m,n \in Z^+$ ، $(m,n)=1$, $m>n$ بحيث أن $m \not\equiv n \pmod 2$

$$x=2mn \ , \ y=m^2-n^2 \ , \ z=m^2+n^2$$

البرهان :

نفرض أن (x,y,z) ثلاثي فيثاغورس بدائي و x عدد زوجي . إذاً y عدد فردي حسب مبرهنة (٧-٢-٣) ، وعليه فإن z فردي حسب مبرهنة (٧-٢-٢)، وبالتالي فإن $x+z \ , \ z-y$ عددان زوجيان ، وعليه يوجد $u,v \in Z^+$ بحيث أن $z+y=2u \ , \ z-y=2v$. لكن $x^2+y^2=z^2$. إذاً

$$x^2=z^2-y^2=(z+y)(z-y)=4uv$$

وعليه فإن $(\frac{x}{2})^2=uv$.

والآن لنفرض أن $(u,v)=d$. إذاً $d\backslash u$ و $d\backslash v$ ، وعليه فإن $d\backslash(u+v)$ و $d\backslash(u-v)$ وهذا يعني أن $d\backslash z$ و $d\backslash y$ ، وعليه فإن $d\backslash(y,z)$. لكن $(y,z)=1$. إذاً $d\backslash 1$ ، وعليه فإن $d=1$.

وحيث أن $u\upsilon=(\frac{x}{2})^2$ و $(u,v)=1$. إذاً يوجد $m,n\in Z$ بحيث أن $u=m^2$, $v=n^2$ حسب مبرهنة (٧-٢-٤) . ولكي نثبت أن $(m,n)=1$ ، نفرض أن $(m,n)>1$. إذاً يوجد عدد أولي p بحيث أن $p\backslash n$, $p\backslash n$ حسب مبرهنة (٢-٢-٤أ) ، وعليه فإن $p\backslash m^2$, $p\backslash n^2$ ، وبالتالي فإن $p\backslash u$, $p\backslash v$ ، وعليه فإن $(u,v)=p>1$ وهذا يناقض كون $(u,v)=1$ إذاً $(m,n)=1$.

وحيث أن $x^2=4uv$ ، $y=u-v$ ، $z=u+v$ ، $u=m^2$ ، $v=n^2$ إذاً $x=2mn$, $y=m^2-n^2$, $z=m^2+n^2$.

وبما أن $(m,n)=1$. إذاً لا يمكن أن يكون m,n زوجين معاً . وإذا كان كل من m,n عدداً فردياً ، فإن ذلك يعني أن كلاً من x,y,z عدد زوجي وهذا يناقض كون $(x,y,z)=1$. إذاً $m\not\equiv n \pmod 2$.

ولإثبات العكس نفرض أن x عدد زوجي و $x=2mn$ ، $y=m^2-n^2$، $z=m^2+n^2$ ، $(m,n)=1$ ، $m\not\equiv n \pmod 2$. إذاً

$$x^2+y^2=4m^2n^2+m^4-2m^2n^2+n^4=(m^2+n^2)^2=z^2$$

ولكي نثبت أن $(x,y,z)=1$ ، نفرض أن $(x,y,z)=d>1$. إذاً يوجد عدد أولي p بحيث أن $p\backslash d$ حسب مبرهنة (٢-٢-٤أ) . لكن $m\not\equiv n \pmod 2$. إذاً $m-n\not\equiv 0 \pmod 2$ و $m+n\equiv 0 \pmod 2$ ، وعليه فإن $y=m^2-n^2=(m+n)(m-n)\equiv 0 \pmod 2$، وبالتالي فإن y عدد فردي، وعليه فإن $p\neq 2$ ، $p\backslash y$ ، $p\backslash z$. إذاً $p\backslash(z+y)$, $p\backslash(z-y)$ ، وعليه فإن $p\backslash 2m^2$ و $p\backslash 2n^2$ ، وبالتالي فإن

$p \backslash m^2 , p \backslash n^2$ ، وعليه فإن $p \backslash m , p \backslash n$ ، ومنها نجد أن $(m,n) = p \neq 1$ وهذا خلاف الفرض . إذاً $(x,y,z) = 1$ ، وعليه فإن (x,y,z) ثلاثي فيثاغورس بدائي .

□

ملاحظة (١) :

إن الشرط $m \not\equiv n \pmod 2$ ضروري في مبرهنة (٧-٢-٥) ، لأنه إذا كان $m = 7, n = 3$ ، فإن $(7,3) = 1$, $7 \equiv 3 \pmod 2$. لكن $x = 2mn = 42 , y = m^2 - n^2 = 40$ ، $z = m^2 + n^2 = 58$ ثلاثي فيثاغورس غير بدائي .

ونورد في الجدول الآتي بعض ثلاثيات فيثاغورس البدائية :

m	n	x	y	z	x^2	y^2	z^2
2	1	4	3	5	16	9	25
3	2	12	5	13	144	25	169
4	1	8	15	17	64	225	289
4	3	24	7	25	576	49	625
5	2	20	21	29	400	441	841
5	4	40	9	41	1600	81	1681
6	1	12	35	37	144	1225	1369
6	5	60	11	61	3600	121	3721
7	2	28	45	53	784	2025	2809
7	4	56	33	65	3136	1089	4225
7	6	84	13	85	7056	169	7225
8	1	16	63	65	256	3969	4225
8	3	48	55	73	2304	3025	5329
8	5	80	39	89	6400	1521	7921
8	7	112	15	113	12544	225	12769

ملاحظة (٢) :

من مبرهنة (٧-٢-١) ومبرهنة (٧-٢-٥) ، نجد أن (x,y,z) ثلاثي فيثاغورس إذاً وإذا فقط وجد $r,s \in Z^+$ ، $r > s > 0$ ، $(r,s) = 1$ ، بحيث أن :

$$x = 2rs \quad , \quad y = r^2 - s^2 \quad , \quad z = r^2 + s^2$$

والآن إلى بعض التطبيقات والأمثلة الآتية .

مثال (٢) :

إذا كان (x,y,z) ثلاثياً فيثاغورسياً بدائياً ، فإن واحد فقط من العددين x أو y يقبل القسمة على 3 .

الحل :

بما أن (x,y,z) ثلاثي فيثاغورسي بدائي . إذاً يوجد $m,n \in Z^+$ ، بحيث أن $(m,n) = 1$ ، $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$. فإذا كان $3 \setminus m$ أو $3 \setminus n$ ، فإن $3 \setminus x$. أما إذا كان $3 \nmid m$ و $3 \nmid n$ ، فإن $m^2 \equiv 1 (\mathrm{mod}\ 3)$ ، $n^2 \equiv 1 (\mathrm{mod}\ 3)$ حسب مبرهنة فيرما ، وعليه فإن $m^2 - n^2 \equiv 0 (\mathrm{mod}\ 3)$ ، وبالتالي فإن $y \equiv 0 (\mathrm{mod}\ 3)$ ، وعليه فإن $3 \setminus y$.

مثال (٣) :

أوجد ثلاثيات فيثاغورس (x,y,z) و $x = 8$

الحل :

بما أن $x = 2mn$. إذاً $mn = 4$. لكن $(m,n) = 1$ ، $m > n > 0$. إذاً $m = 4$, $n = 1$ ، وعليه فإن $y = 4^2 - 1^2 = 15$, $z = 4^2 + 1^2 = 17$ و $(8,15,17)$ ثلاثي فيثاغورس بدائي . لكن $x = ad$ ، $y = bd$ ، $z = ed$ حيث (a,b,c) ثلاثي فيثاغورس بدائي . إذاً $a \setminus 8$ ، وعليه فإن $a = 1,2,4,8$. فإذا كان أحد هذه القواسم عدداً من ثلاثي بدائي ، فيجب أن يكون على الصورة $a = 2rs$ حسب مبرهنة (٧-٢-٥) . لكن $2rs \neq 1$ كما أن $2rs = 2$ يعني أن $rs = 1$ ، وبالتالي فإن $r = s = 1$ وهذا غير ممكن لأن $r > s > 0$.

أما إذا كان $2rs = 4$ ، فإن $rs = 2$ ، وعليه فإن $r = 2 , s = 1$ ، وبالتالي فإن $a = 4 , b = r^2 - s^2 = 3 , c = b^2 + r^2 = 5$ ، وعليه فإن $(4,3,5)$ ثلاثي فيثاغورس بدائي ، وبضرب كل عدد من أعداد هذا الثلاثي في 2 نجد أن $(8,6,10)$ ثلاثي فيثاغورس .

أما إذا كان $2rs = 8$ ، فإن $rs = 4$ ، وعليه فإن $r = 4 , s = 1$ ، وبالتالي فإن $x = 8 , y = 15 , z = 17$. إذاً الثلاثيات المطلوبة هي $(8 , 6 ,10)$ ، $(8 , 15 , 17)$.

مثال (٤) :

أوجد ثلاثيات فيثاغورس البدائية $(x,21,z)$.

الحل :

بما أن $y = 21$ ، $y = m^2 - n^2$. إذاً $(m^2 - n^2) = 21$ ، وعليه فإن $(m + n)(m - n) = 21$. إذاً إما $m + n = 21$ ، $m - n = 1$ أو $m + n = 7$ و $m - n = 3$ ، وعليه إما $m = 11$ ، $n = 10$ أو $m = 5$ ، $n = 2$ ، وعليه إما $x = 2mn = 220 , z = m^2 + n^2 = 221$ أو $x = 2 \cdot 2 \cdot 5 = 20 , z = 5^2 + 2^2 = 29$ ، وبالتالي فإن الثلاثيات البدائية المطلوبة هي $(20 ,21 , 29)$ ، $(220 , 21 , 221)$.

مثال (٥) :

أوجد ثلاثيات فيثاغورس البدائية $(x, y,65)$.

الحل :

بما أن $z = 65$ ، $y = m^2 + n^2$. إذاً $m^2 + n^2 = 65 = 8^2 + 1^2$ أو $m^2 + n^2 = 65 = 7^2 + 4^2$ ، وعليه إما $(m^2 = 8^2 ,n^2 = 1)$ أو $(m^2 = 7^2 , n^2 = 4^2)$ ومنها نجد أن $m = 8 , n = 1$ أو $m = 7 , n = 4$.

فإذا كان $m = 8 , n = 1$ ، فإن $y = m^2 - n^2 = 63$ و $x = 2mn = 16$ و $(16 , 63 , 65)$ ثلاثي فيثاغورس .

وإذا كان $m = 7 , n = 4$ ، فـإن $x = 56 , y = 33 , z = 65$ ، وعليـه فـإن $(56 , 33 , 65)$ ثلاثي فيثاغورس .

وحيث أن $65 = 5 \cdot 13$. إذاً القواسم الفعلية للعددي هـي $1,5,13$ ، فـإذا كـان (a,b,c) ثلاثي فيثاغورس بدائي ، فإن $c \neq 1$. إذاً $c = 5 ,13 , 65$. فإذا كان $c = 5$، فإن $r^2 + s^2 = 5 = 2^2 + 1$ ، وعليه فإن $r = 2$، $s = 1$ ، وبالتالي فـإن $a = 4 , b = 3$ و $(4, 3, 5)$ ثلاثي فيثاغورس بدائي وبضرب عناصره في 13 ينتج أن $(65 , 39 , 52)$ ثلاثي فيثاغورس .

وإذا كان $c = 13$ ، فإن $c = r^2 + s^2 = 9 + 4$ ، وعليه فـإن $r = 3$، $s = 2$ ، وبالتالي فإن $a = 12 , b = 5$ ، وعليه فـإن $(13 , 5 , 12)$ ثلاثـي فيثـاغورس بدائي ، وبضرب عناصره في 5 نجد أن $(65 , 25 , 60)$ ثلاثي فيثاغورس . إذاً ثلاثيات فيثاغورس المطلوبة هي

$$(16 ,63 , 65) \ , \ (56 , 33, 65) \ , (52,39,65) \ , (60,25,65)$$

<u>مثال (٦) :</u> " الخازن "

أوجد الأعداد الصحيحة الموجبة التي تحقق المعادلة $x^2 + y^2 = z^4$.

<u>الحل :</u>

نفرض أن $r = z^2$. إذاً $x^2 + y^2 = r^2$ ، وعليه إذا فرضنا أن (x,y,r) ثلاثي فيثاغورس بدائي ، فإن

$$x = 2mn \ , \ y = m^2 - n^2 \ , \ r = m^2 + n^2$$

لكن $r = z^2$. إذاً $m^2 + n^2 = z^2$ ، وعليه يوجد $u,v \in Z$ ، بحيث أن

$$m = 2uv \ , \ n = u^2 - v^2 \ , \ z = u^2 + v^2$$

وعليه فإن حلول المعادلة $x^2 + y^2 = z^4$ هي

$$x = 4uv\,(u^2 - v^2) \ , \ y = 4u^2v^2 - (u^2 - v^2) \ , \ z = u^2 + v^2 ،$$

$$u,v \in Z \ , \ u > v \ ، \ (u,v) = 1 \ .$$

فإذا كان $u=2\,,\ v=1$ ، فإن $z=5 \quad , \quad y=7 \quad , \quad x=24$

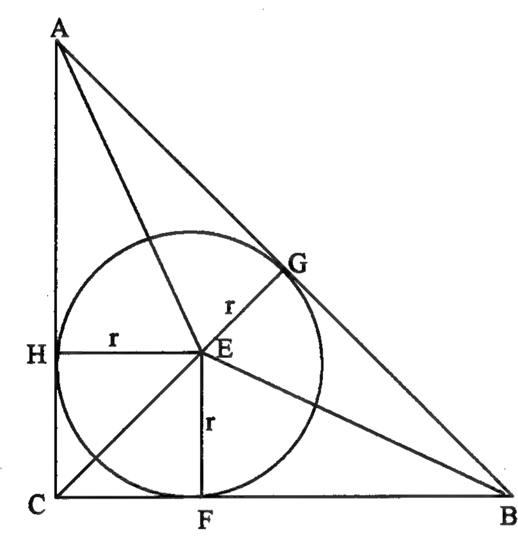
وإذا كان $u=3\,,\ v=2$ ، فإن $z=13 \quad , \quad y=119 \quad , \quad x=120$

وإذا كان $u=4\,,\ v=3$ ، فإن $z=25 \quad , \quad y=527 \quad , \quad x=336$

<u>مثال (٧) :</u>

أثبت أن نصف قطر الدائرة المرسومة داخل مثلث فيثاغورس (مثلث قائم الزاوية أطوال أضلاعه أعداد صحيحة) يكون عدداً صحيحاً

<u>الإثبات :</u>



نفرض أن نصف قطر الدائرة يساوي r ، $|AB|=c\,,\ |AC|=b$ ، $|BC|=a$. إذاً $a^2+b^2=c^2$.
وحيث مساحة المثلث تساوي نصف القاعدة في الإرتفاع ، والمماس عمودي على نصف القطر عند نقطة التماس ، ومساحة المثلث ABC تساوي مجموع مساحات المثلثات ACE ،ABE ،BCE "أنظر الشكل"

إذاً $\frac{1}{2}ab=(\frac{1}{2}br+\frac{1}{2}cr+\frac{1}{2}ar)$ ، وعليه فإن

$$ab=(a+b+c)\,r \qquad \ldots (1)$$

لكن $a^2+b^2=c^2$ يعني وجود $s,t\in Z$ بحيث أن $s>t$ ،

$$a=2st\ ,\ b=s^2-t^2\ ,\ c=s^2+t^2 \qquad \ldots (2)$$

ومن (1) ، (2) ينتج أن

$$r=\frac{ab}{a+b+c}=\frac{2st\,(s^2-t^2)}{2st+2s^2}=\frac{t\,(s^2-t^2)}{s+t}=t\,(s^2-t^2)\in Z^+$$

تمـــــارين

(١) أوجد ثلاثيات فيثاغورس البدائية (x,y,z) عندما :

(أ) $x=16$ ، (ب) $y=35$ ، (ج) $z=145$

" لاحظ أن $145=(12^2)+1=9^2+8^2$ "

(٢) أوجد ثلاثيات فيثاغورس (x,y,z) عندما :

(أ) $x=4$ ، (ب) $y=45$ ، (ج) $z=85$

" لاحظ أن $85=81+4=49+36$ "

(٣) " الخازن " أوجد حلول المعادلة $x^4+y^2=z^2$.

(٤) إذا كان $x^2+y^2=z^2$ ، فأثبت أن واحداً من الأعداد x,y,z يقبل القسمة على 3 وواحداً يقبل القسمة على 5 .

(٥) إذا كـــان (x,y,z) ثلاثيـــاً فيثاغورســـياً بـــدائياً ، فأثبـــت أن $12 \backslash xy$ و $60 \backslash xyz$.

(٦) إذا كان (x,y,z) ثلاثياً فيثاغورسياً بدائياً ، فأثبــت أن $x+y$ و $x-y$ يطابق الواحد أو السبعة قياس 8 .

(٧) إذا كان $n\geq 3$ ، فأوجد ثلاثياً فيثاغورسياً يكون أحد أعــداده يــساوي n .

" ملاحظة : إذا كان n عدداً زوجياً فخذ $\frac{n^2}{4}+1 , \frac{n^2-1}{4}-1, n$ تحــصل على المطلوب . وإذا كان n عدداً زوجياً فخذ $\frac{n^2+1}{2} , \frac{n^2-1}{2} , n$ تحصل على المطلوب " .

(٨) " الخازن " برهن على عدم وجــود ثلاثــي فيثاغورســي (x,y,z) فيــه $x=2^m , y=2^n , m>n$.

(٩) برهن أن $(3,4,5)$ هو الثلاثي الفيثاغورسي البدائي الوحيد المكون من ثلاثة أعداد صحيحة متتالية .
" ملاحظة : أفرض وجود ثلاثي بالشكل $(x, x+1, x+2)$ "

(١٠) أثبت أن $(3n, 4n, 5n)$ ، $n = 1, 2, 3, \dots$ هي الثلاثيات الفيثاغورسية الوحيدة التي تكوّن أعدادها متوالية عددية .
"ملاحظة : أفرض أن $(x-n, x, x+n)$ ثلاثي فيثاغورس ، ثم أوجد x بدلالة n تحصل على المطلوب " .

(١١) إذا كان (x,y,z) ثلاثياً فيثاغورسياً بدائياً ، وكان $z = x+1$ ، فأثبت أن $x = 2n(n+1)$, $y = 2n+1$, $z = 2n(n+1)+1$ " لاحظ أن $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, $z - x = 1 \Rightarrow m = n+1$

(١٢) إذا كان (x,y,z) ثلاثياً فيثاغورسياً بدائياً ، وكان $z - y = 2$ ، فأثبت أن $x = 2m$, $y = m^2 - 1$, $z = m^2 + 1$ ، $m > 1$.

(١٣) أوجد جميع مثلثات فيثاغورس التي مساحتها تساوي محيطها ." لاحظ أن $(x^2 + y^2 = z^2 \; , x + y + z = \frac{1}{2}xy) \Rightarrow (x-4)(y-4) = 8$" .

(١٤) إذا كان $(x,y,z) = 1$ ، فأوجد حلول المعادلة $2x^2 + y^2 = z^2$.

٧-٣ : حالات خاصة من مبرهنة فيرما الأخيرة

Special cases of Fermats Last theorem

تنص مبرهنة الفرنسي فيرما (١٦٠١-١٦٦٥م) على عدم وجود أعداد صحيحة غير صفرية x, y, z تحقق المعادلة الديوفنتية

$$x^n + y^n = z^n \qquad \dots (1)$$

ويقول فيرما أنه توصل إلى هذه الحقيقة سنة ١٦٣٧م عندما كان يقرأ طبعة باشيه لأعمال ديوفنتس ولدية إثبات لذلك لكن ضيق الهامش منعه من كتابته ، لكن

جميع الأبحاث في التراث العلمي العربي والإسلامي ، أنظر [٣،٤،٥] ، تؤكد بأن الرياضيين المسلمين كانوا على علم بهذه المبرهنة عندما $n = 3,4$ ، فمنذ القرن العاشر للميلاد حاول كل من أبو بكر الكرخي (ت ١٠٢٠م) وأبو محمود الخجندي (ت١٠٠٠م) إثبات مبرهنة فيرما عندما $n = 3$ ، أي عدم وجود أعداد صحيحة غير صفرية x, y, z بحيث أن $x^3 + y^3 = z^3$ وبلغة ذلك العصر " **لا يجتمع من عددين مكعبين عدد مكعب** " .

ولكن أبو جعفر الخازن أحد رياضي القرن العاشر للميلاد يؤكد بأن برهان الخجندي ناقص وغير صحيح ، ثم يحاول الخازن أن يبرهن القضية الآتية " **لا يمكن أن يجتمع من عددين مكعبين عدد مكعب كما قد يمكن أن يجتمع من عددين مربعين عدد مربع ، ولا أن ينقسم عدد مكعب إلى عددين مكعبين ، كما قد ينقسم عدد مربع إلى عددين مربعين** " ويبدأ برهانه بإثبات المتطابقة الآتية .

كل عددين مكعبين ، فإن فضل ما بينهما هو الذي يجتمع من ضرب مربع الضلع الأقل في فضل ما بين الضلعين ومن ضرب مجموع الضلعين في فضل ما بينهما ثم في الضلع الأكبر .

أي أنه إذا كان $z > y$ ، فإن $z^3 - y^3 = y^2(z - y) + (z + y)(z - y)z$ ، وحيث أن الطرف الأيمن من المتطابقة أعلاه يقابل حجماً لكنه ليس مكعباً لأنه لم يجتمع من ضرب عدد مربع في ضلعه . إذاً لا ينقسم عدد مكعب إلى مكعبين ، لأنه إذا فرضنا وجود عددين مكعبين ضلعاهما $|bc|$ ، $|ab|$ ، وكان $|bc| > |ab|$ ، $|ab| + |bc| = |bd|$ ، فإن $|bd| > |bc|$. إذاً إذا كان $|bd|$ ضلع مكعب فإنه إذا نقص من مكعبه مكعب $|bc|$ بقى الباقي مثل مكعب $|ab|$ ، ولكن الفرق بين مكعبين ليس مكعباً ، كما أوضحنا أعلاه . إذاً $|bd|$ ليس بضلع مكعب ولا مجموع مكعبي $|ab|$ ، $|bc|$ بعدد مكعب .

لاحظ أن برهان الخازن ناقص أيضاً واعتماده على التعليل الهندسي للمطابقة أعلاه لا يؤدي إلى التعميم لأن الحالة $n = 4$ لا يمكن إعطائها تفسيراً هندسياً .

أما في القرن الحادي عشر للميلاد فقد ذكر ابن سينا (٩٨٠-١٠٣٧م) في كتابه " الشفاء : المنطق – البرهان " أن هذه المبرهنة " أي $z^3 + y^3 = z^3$ لم يتم البرهان عليها ، أما في القرن الثاني عشر للميلاد فنجد عمر الخيام (١٠٤٨-١١٣١م) يذكر دون إثبات استحالة وجود أعداد صحيحة غير صفرية a, b, c بحيث أن $x^3 + y^3 = z^3$ أو $x^4 + y^4 = z^4$.

أما في القرن الثالث عشر للميلاد فيطرح ابن الخوام البغدادي (١٢٤٥-١٣٢٤م) بعض المعادلات الديوفنتية التي منها معادلة فيرما عندما $n = 3$ ، وكذلك يفعل كمال الدين الفارسي في شرحه لجبر ابن الخوام ، أما بهاء الدين العاملي (١٥٤٧-١٦٢٢م) فقد ذكر في كتابه "خلاصة الحساب" استحالة تقسيم المكعب إلى مكعبين أو ضعف المربع إلى مربعين ، وقد جاءت ملاحظة فيرما بعد وفاة العاملي بحوالي خمسة عشر عاماً .

هذا ولقد أثبت فيرما بطريقته التي تعرف بطريقة النزول أو الانحدار أو التناقص اللانهائي Descente infinie، كما أثبت كل من أويلر(١٧٠٧-١٧٨٣) وجاوس (١٧٧٧-١٨٥٥) عدم وجود حل في Z للمعادلة $x^4 + y^4 = z^4$, $xyz \neq 0$ وعليه إذا كان $n > 2$, $4 \backslash n$ ، فإن $n = 4m$ ، وبالتالي فإن $(x^m)^4 + (y^m)^4 = (z^m)^4 \Leftrightarrow x^n + y^n = z^n$

لكن $(x^m)^4 + (y^m)^4 = (z^m)^4$ لا تملك حلاً غير تافه في Z . إذاً $x^n + y^n = z^n$ لا تملك حلاً في Z لكل $n = 4m$ بشرط أن $xyz \neq 0$.

أما إذا كان $n = 3$ ، فقد أثبت أويلر سنة ١٧٧٠م صحة المبرهنة في هذه الحالة، لكن إثبات أويلر يحتوي على بعض الأخطاء صححت من قبل لجندر

(١٧٥٢-١٨٣٣) ، وأثبت جاوس (١٧٧٧-١٨٥٥م) هذه الحالة بإستخدام خواص الحقـــل $Q(\sqrt{-3})$ أمـــا الفرنـــسية صـــوفي جيرمـــا (١٧٧٦-١٨٣١ Sophie Germain)، فقد أثبتت سنة ١٨٢٠م صحة المبرهنـــة $x^n + y^n = z^n$ لكل $n > 100$ بشرط أن كلاً من $n, 2n+1$ عدد أولي ، كما أن كلاً من x, y, z لا يقبل القسمة على n ، ثم وسع لجندر طريقتها لكل الأعداد الأقـل مـن 197 ، وأثبت عام ١٨٢٣م أن n لا يمكن أن تكون على الصورة

$$2p+1 , 3p+1 , 8p+1 , 10p+1 , 14p+1 , 16p+1$$

حيث n,p أعداد أولية ، $n \neq 31 , 43$.

وبإستخدام طريقة النزول اللانهائي أثبت الألماني ديركلي (١٨٠٥-١٨٥٩) سنة ١٨٢٨م صحة المبرهنة عندما $n = 5$ ، كما أثبت ذلك لجنـدر سـنة ١٨٣٠م ، وأثبت ديركلي سنة ١٨٣٢م صحة المبرهنة عندما $n = 14$ ، وفي سـنة ١٨٣٩م قدم الفرنسي لامي (١٧٩٥-١٨٧٠ , Gabriel Lame) برهاناً عندما $n = 7$ ، لكنه يحتوي على بعض الأخطاء صححت من قبل الفرنـسي لبيـك Lebesgue (١٨٧٥-١٩٤١) سنة ١٨٤٠م .

وفي ١٨٤٧/٣/١م أبلغ لامي أكاديمية العلوم الفرنسية في باريس أنـه أثبـت مبرهنة فيرما معتبراً أن

$$x^p + y^p = (x + y)(x + \zeta y) \cdots (x + \zeta^{p-1} y) \in Z[\zeta_p]$$

حيث $\zeta_p = e^{\frac{2\pi i}{p}}$ ، $p \neq 2$ ، $Z[\zeta_p] = \{a + b\zeta_p | a, b \in Z\}$ منطقة تحليل وحيـد (unique factorization domain) ، لكـن الفرنـسي ليـوفيلي (١٨٠٩-١٨٨٢) لم يقتنع ببرهان لامي ، وبعد عدة أشهر أكتشف الفرنسي كوشي (١٧٨٩-١٨٥٧) أن $Z[\zeta_{23}]$ منطقة ليست وحيدة التحليل .

هذا وقد أثبت الألماني كومر (١٨١٠-١٨٩٣) صحة مبرهنة فيرما الأخيـرة

لكل الأعداد الأولية المنتظمة p (Regular Primes) الأقـل مـن 100 ماعـدا $p = 37 , 59,67$ " يقال عن عدد أولي أنه منتظم إذا كان p لا يقسم مقام أي من أعـداد برنـولي $B_2, B_4, \cdots, B_{p-3}$ حيـث B_n معرفـة بالـشكل $\frac{x}{e^x - 1} = 1 + \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$. وقد منح كومر على ذلك الميدالية الذهبية مـن قبـل أكاديمية العلوم الفرنسية سنة ١٨٥٠م .

وأثبت الروسي فيريمانوف سـنة ١٨٩٣م صـحة المبرهنـة فيرمـا عنـدما $n = 37$، ثم أثبت في ١٩٥٥م صحة تلك المبرهنة لكل $n \le 257$.

وأثبت ڤايفريش (Wieferich) فـي ١٩٠٩م أنـه إذا وجـد حـل للمعادلـة $x^n + y^n = z^n$ وكل من x, y, z لا يقبل القسمة على n (والتي تـسمى الحالـة الأولى من مبرهنة فيرما) ، فإن $2^n \equiv 2 (\text{mod } n^2)$ و n عدد أولي .

ثم أثبـت كـل مـن ميريمـانوف وفـروبينيص (Frobenios) و ڤانـديڤر (Vandiver) وپولكزك (Pollackzek) و موريشيما (Morishima) وروسـر (Rosser) أنه إذا وجد حل للحالة الأولى من مبرهنة فيرما الأخيرة فإن

$$q = 3,5,7,11,17,19\ 23,29,31,37,41,43 \ ، \ q^n \equiv q \ (\text{mod } n^2)$$

وبإستخدام تلك النتائج أثبت الفرنسي لمير (Lehmers) صحة الحالة الأولى من مبرهنة فيرما لكل الأعداد الأولية $n < 2537\ 47889$.

وفـي سـنة ١٩٥٥م وضـع اليابانيـان شـيمورا و تانيامـا تخمينـاً (Shimura – Taniyama Conjecture) حول المنحنيات الجبرية الأهليلجيـة أو الناقصة (Elliptic curves) وهي منحنيات من النـوع $y^2 = ax^3 + bx + c$ **ينص على أن " كل المنحنيـات الناقـصة علـى Q منحنيـات أوليـة أو قياسـية (Modular curves) .**

وفي سنة ١٩٨٣م أثبت فلاتنج (Flatings) ، أن لكـل $n > 2$ يوجـد علـى الأكثر عـدد منتهـي مـن الأعـداد الأوليـة نـسبياً مـع x, y, z بحيـث أن $x^n + y^n = z^n$. لكن فلاتنج لم يستطع أن يثبت في جميع الحالات بأن هذا العدد المنتهي هو الصفر .

وفي سنة ١٩٨٥ وضّح فري (Fery) العلاقة بين تخمـين شـيمورا – تانيامـا ومبرهنة فيرما الأخيرة بإثباته أمكانياً إيجاد أو بناء منحنى ناقص غيـر قياسـي سُميّ فيما بعد منحنى فري (Frey curve) . لاحظ أن فري لم يبرهن علـى أن هذا المنحنى غير قياسـي (not modular) ، بـل أثبـت ذلـك كـين ريبـت (Ken Ribet) من بركلي منح عليه جائزة فيرما سنة ١٩٨٩م .

وفي سنة ١٩٨٧م أقترح الفرنسي سار (Serre) وصفاً عاماً لجميع تمثـيلات زمر جالوا الثنائية البعد على الحقول المنتهية بدلالة الأشكال أو الدوال المـستدقة أو الهلالية (cusp form) " نوع خاص من الدوال يـضمحل عنـد المالانهايـة $(f(\infty) = 0)$ " . ثم وضع التخمين الآتي (Serre conjecture) :

كل تمثيل غير قابـل للتحليـل (irreducible Representation) مـن الـشكل $f(z) = \sum_{n=1}^{\infty} a(n) e^{2n\pi iz}$ ، $a(1) = 1$ يكون قياسياً .

وبين سار أن صحة هذا التخمين تثبت صحة تخمين شيمورا – تانياما من جهـه ، كما يثبت صحة مبرهنة فيرما الأخيرة .

وفي سنة ١٩٩٣م أثبت الإنجليزي أندرو ويلـس (A. Wiles) صـحة حـدس شيمورا – تانيانا للمنحنيات الناقصية شـبه المـستقرة (Semi-stable curves) وأثبت صحتها بصورة عامة ، ريبت من بركلي سنة ١٩٩٩م ، وفي سنة ١٩٩٤م وبمساعدة الإنجليزي تيلور (R. Taylor) من كمبـرج ، أثبـت ويلـس صـحة مبرهنة فيرما الأخيرة ومنح على ذلك ميدالية فيلد في الرياضيات سنة ١٩٩٥م .

وسنركز أهتمامنا في هذا الجزء على إثبات مبرهنة فيرما الأخيرة لكل $4 \setminus n$ ، إضافة إلى الحالة $x^3 + y^3 = z^3$.

٧-٣-١ : المعادلة $x^4 + y^4 = z^4$.

لكي نثبت مبرهنة فيرما لكل $4 \setminus n$ نثبت أن $x^4 + y^4 = z^4$ لا تملك حلاً في Z^+ ، بإستخدام طريقة فيرما " طريق الإنحدار أو النزول اللانهائي (Infinite Descent) والتي تتلخص بما يأتي :

لإثبات استحالة علاقة على مجموعة الأعداد الطبيعية N ، نفرض وجود مجموعة $\phi \neq S \subseteq N$ تحقق تلك العلاقة ، إذاً S تحوي عنصر أصغر a ثم نبرهن على وجود عنصر آخر في S أصغر من a فنحصل على تناقض وبذلك يتم البرهان .

والآن إلى المبرهنة الآتية .

مبرهنة ٧-٣-١ :

لا يوجد حل في Z للمعادلة الديوفنتية

$$x^4 + y^4 = z^2 \quad ، \quad xyz \neq 0 \qquad \dots (1)$$

البرهان :

لإثبات عدم وجود حل للمعادلة (1) في Z ، يكفي أن نبرهن على عدم وجود حل لها في Z^+ . ولإثبات ذلك نفرض أن

$$S = \{z \in Z \mid x^4 + y^4 = z^2 \ , \ x, y \in Z^+\} \neq \phi$$

إذاً S مجموعة جزئية غير خالية من N ، وعليه فإن S تحوي عنصر أصغر مثل u حسب قاعدة الترتيب الجيد . إذاً $x^4 + y^4 = u^2$.

يمكن أن نفرض أن $(x,y,u)=1$ ، لأنه إذا كان $(x,y,u)\neq 1$ نقسم علي القاسم المشترك الأعظم للأعداد x,y,u ، فتتحول إلى أعداد أوليه نسبياً.

إذاً $(x,y)=1$ ، وعليه فإن واحداً منها عدد فردي ، وبالتالي فإن

$$u^2 = x^4 + y^4 \equiv 1 (\bmod 4) \text{ أو } u^2 = x^4 + y^4 \equiv 2 (\bmod 4)$$

لكن $u^2 \not\equiv 2(\bmod 4)$ ، لكل $u \in Z_4^* = \{1,2,3\}$. إذاً $u^2 \equiv 1(\bmod 4)$ ، وعليه فإن u عدد فردي ، وأما x أو y عدد زوجي . فإذا فرضنا أن x عدد زوجي ، فإن (x^2, y^2, u) ثلاثي فيثاغورس بدائي وعليه يوجد $a,b \in Z^+$ ، بحيث أن $a > b > 0$ ، $(a,b)=1$ ، $a \not\equiv b(\bmod 2)$

$$x^2 = 2ab \ , \ y^2 = a^2 - b^2 \ , \ u = a^2 + b^2 \text{ حسب مبرهنة (٧-٢-٥)}$$

والآن إذا كان a عدداً زوجياً و b عدداً فردياً ، فإن $y^2 \equiv -1(\bmod 4)$ وهذا غير ممكن . إذاً a عدد فردي و b عدد زوجي ، وعليه فإن $b = 2c$ ، وبالتالي فإن $x^2 = 4ac$ ، وعليه فإن $(\frac{x}{2})^2 = ac$ ، $(a,c)=1$. إذاً يوجد $e,d \in Z^+$ ، بحيث أن $a = d^2 \ , c = e^2$ ، $(d,e)=1$ حسب مبرهنة (٧-٢-٤) ، إذاً d عدد فردي ، وعليه فإن $u = a^2 + b^2 \ , \ y^2 = a^2 - b^2 = d^4 - 4e^4$ ، ومنها نجد أن $(2e^2) + y^2 = (d^2)^2$ ، كما أن $(2e^2, y, d^2) = 1$ ، وعليه يوجد $m,n \in Z^+$ ، بحيث أن $m > n$ ، $(m,n)=1$ ، $2e^2 = 2mn \ , d^2 = m^2 + n^2$.

لكن $e^2 = mn$ ، $(m,n)=1$. إذاً يوجد $r,s \in Z^+$ ، بحيث أن $m = r^2 \ , n = s^2$ حسب مبرهنة (٧-٢-٤) ، وعليه فإن $r^4 + s^4 = d^2$. لكن $d \leq d^2 = a \leq a^2 < a^2 + b^2 = u$ و $d \in S$ وهذا يناقض كون u عنصر أصغر في S . إذاً $S = \phi$ ، وعليه لا يوجد حل للمعادلة $x^4 + y^4 = z^2$ في Z^+ .

□

نتيجة (١) :

لا يوجد حل في Z للمعادلة $x^4 + y^4 = z^4$ ، $xyz \neq 0$.

البرهان :

نفرض أن $a,b,c \in Z$ حـــل للمعادلـــة $x^4 + y^4 = z^4$. إذاً a,b,c^2 حـــل للمعادلة $x^4 + y^4 = z^2$ وهذا يناقض مبرهنـــة (٧-٣-١) . إذاً لا يوجـــد حـــل للمعادلة $x^4 + y^4 = z^4$ في Z .

□

نتيجة (٢) :

إذا كان $4 \setminus n$ ، فلا يوجد حل في Z للمعادلة $x^n + y^n = z^n$ ، $xyz \neq 0$.

البرهان :

بما أن $m = 4m$ ، $m \geq 1$. إذاً $x^n + y^n = z^n \Leftrightarrow (x^m)^4 + (y^m)^4 = (z^m)^4$ وعليـــه إذا كـــان $a,b,c \in Z$ حـــلاً للمعادلـــة $x^n + y^n = z^n$ ، فـــإن $a^m, b^m, c^m \in Z$ حل للمعادلة $x^4 + y^4 = z^4$ وهذا يناقض نتيجة (١) . إذاً لا يوجد حل في Z للمعادلة $x^n + y^n = z^n$ ، $xyz \neq 0$.

□

مبرهنة ٧-٣-٢ :

لا يوجد حل في Z للمعادلة

$$x^4 - y^4 = z^2 \quad , \quad xyz \neq 0 \qquad \ldots (2)$$

البرهان :

يكفي أن نبرهن على عدم وجود حل للمعادلة (2) في Z^+ ، ولإثبات ذلك نفرض أن $S = \{x \in Z^+ \mid x^4 - y^4 = z^2 \quad , \quad y,z \in Z^+\} \neq \phi$. إذاً S مجموعـــة جزئية غير خالية من N ، وعليه فإن S تحوي عنصر أصـــغر ولـــيكن u حـــسب قاعدة الترتيب الجيد . إذاً $u^4 - y^4 = z^2$ ، وعليه فإن $u^4 = y^4 + z^2$

والآن إذا كان $(u,y)=d>1$ ، فإن $u=du_1 , y=dy_1$ ، وعليه فإن $d^4(u_1^4-y_1^4)=z^2$ ، وبالتالي فإن $d^2 \setminus z$ ، وعليه فإن $z=d^2z_1$ ، $z_1 \in Z^+$ إذاً $u_1,y_1,z_1 \in Z^+$ حل للمعادلة (2) و $u_1<u$ ، $u_1 \in S$ ، وهذا تناقض . إذاً $(u,y)=1$ و y عدد زوجي أو y عدد فردي .

(أ) إذا كان $(u,y)=1$ و y عدداً زوجياً ، فإن

$(u^2,y^2)=1$ ، $(u^2)^2=(y^2)^2+z^2 \Leftrightarrow u^4=y^4+z^2$. إذاً (y^2,z,u^2) ثلاثي فيثاغورس بدائي ، وعليه يوجد $r,s \in Z^+$ ، $(r,s)=1$ ، $r>s$ ، $r \not\equiv s \pmod 2$ ، $y^2=2rs , z=r^2-s^2 , u^2=r^2+s^2$ حسب مبرهنة (٧-٢-٥) . فإذا كان r زوجياً ، فإن s فردي . لكن $y^2=2rs$ ، $(2r,s)=1$. إذاً يوجد $a,b \in Z^+$ ، بحيث أن $2r=a^2$ ، $s=b^2$ حسب مبرهنة (٧-٢-٤) . لكن a عدد زوجي . إذاً $a=2c$ ، $c \in Z^+$ ، وعليه فإن $r=2c^2$ ، وبالتالي فإن $u^2=r^2+s^2=(2c^2)^2+(b^2)^2$ و $(2c^2,b^2,u)$ ثلاثي فيثاغورس بدائي . إذاً يوجد $m,n \in Z^+$ ، $(m,n)=1$ ، $m>n$ ، $m \not\equiv n \pmod 2$ بحيث أن $2c^2=2mn , b^2=m^2-n^2 , u=m^2+n^2$ لكن $c^2=mn$ ، $(m,n)=1$ يعني وجود $e,f \in Z^+$ ، بحيث أن $m=e^2 , n=f^2$ حسب مبرهنة (٧-٢-٤) ، وعليه فإن $b^2=e^4-f^4$ وهذا يعني أن $x=e$ ، $y=f$ ، $z=b$ حل للمعادلة (2) . لكن $e \in S$, $e=\sqrt{m}<m^2+n^2=u$ يناقض قاعدة الترتيب الجيد . إذاً لا يوجد حل في الحالة .

(ب) إذا كان $(u,y)=1$ و y عدداً فردياً ، فإن $(u^2,y^2)=1$ و $(u^2)^2=z^2+(y^2)^2$ ، (z,y^2,u^2) ثلاثي فيثاغورس بدائي . إذاً يوجد $m,n \in Z^+$ ، $m>n$ ، $(m,n)=1$ ، $m \not\equiv n \pmod 2$ بحيث أن $u^2=m^2+n^2 , y^2=m^2-n^2 , z=2mn$ ، وعليه فإن

$m^4 - n^4 = (m^2 - n^2)(m^2 + n^2) = (yu)^2$ ، وهذا يعني أن $x = m$ ،
$y = n$ ، $z = uy$ حل للمعادلة (2) ، كما أن $x = m < \sqrt{m^2 + n^2} = u$
وهذا يناقض قاعدة الترتيب الجيد . إذاً لا يوجد حل للمعادلة (2) .

□

نتيجة :

مساحة مثلث فيثاغورس ليست مربعاً كاملاً .

البرهان :

نفرض أن x,y طولا ضلعي مثلث فيثاغورس و z طول وتره . ولنفرض أن مساحة هذا المثلث تساوي A . إذاً $A = \frac{1}{2}xy$. والآن لنفرض وجود $u \in Z^+$ بحيث أن $A = u^2$. إذاً $xy = 2u^2$ ، وعليه فإن $2xy = 4u^2 = (2u)^2$.

لكن $x^2 + y^2 = z^2$. إذاً

$$x^2 - 2xy + y^2 = z^2 - 2xy \Leftrightarrow (x-y)^2 = z^2 - (2u)^2$$

$$x^2 + 2xy + y^2 = z^2 + 2xy \Leftrightarrow (x+y)^2 = z^2 + (2u)^2$$

وعليه فإن $(x-y)^2 (x+y)^2 = (x^2 - y^2)^2 = z^4 - (2u)^4$ ، ومنها نجد أن $a = z$, $b = 2u$, $c = x^2 - y^2$ حل للمعادلة $a^4 - b^4 = c^4$ وهذا يناقض مبرهنة (٧-٣-٢) . إذاً $A \neq u^2$.

□

٧-٣-٢ : المعادلة $x^3 + y^3 = z^3$ ، $xyz \neq 0$

لكي نبرهن على عدم وجود أعداد صحيحة غير صفرية x,y,z بحيث أن $x^3 + y^3 = z^3$ نحتاج إلى المفاهيم الآتية : الحقلة والحقل ، الأعداد الجبرية ، العناصر القابلة للإنعكاس ، العناصر المترادفة والعناصر الاولية في حلقة ، ونبدأ بالآتي :

تعريف ٧-٣-١ :

إذا كانت G مجموعة غير خالية و * عملية ثنائية معرفة عليها ، فيقال عن $(G,*)$ أنها زمره (Group) ، إذا كان :

(أ) * عمليـــة تجميعيـــة أو دامجـــة (Associative) . أي أن $(a*b)*c=a*(a*c)$ لكل $a,b,c\in G$.

(ب) يوجد $e\in G$ بحيث أن $a*e=e*a=a$ لكل $a\in G$ يسمى e العنصر المحايد (Tdentity element) .

(ج) لكل $a\in G$ يوجد $b\in G$ بحيث أن $a*b=b*a=e$ يسمى b معكوس أو نظير (Inverse) a ويرمز له بالرمز a^{-1} .

ويقال عن زمره $(G,*)$ أنها إبدالية أو آبليـــة (Abeliam or Commatative) إذا كان $a*b=b*a$ لكل $a,b\in G$.

مثال (١) :

(أ) كل من $(Z,+)$ ، $(R,+)$ ، $(Q,+)$ ، $(R^*,\cdot)$ ، $(Q^*,\cdot)$ ، $(C^*,\cdot)$ زمره إبدالية .

(ب) كل من $(N,+)$ ، $(Z,\cdot)$ ، ليس زمره .

(ج) إذا كان $G=(Z_n,\oplus)$ حيث $[a]\oplus[b]=[a+b]$ لكل $[a],[b]\in Z_n$ ، فإن G زمره إبدالية .

(د) $G=\left(\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d\in R \ , ad-bc\neq 0\right\},\cdot\right)$ حيث . هي عملية ضرب المصفوفات ، فإن G زمره ليست إبدالية .

تعريف ٧-٣-٢ :

إذا كان R مجموعة غير خالية ، $+,\cdot$ عمليتين ثنائيتين معرفتين على R ، فيقال عن $(R,+,\cdot)$ أنها حلقة (Ring) ، إذا كانت :

(أ) $(R,+)$ زمره إبدالية .

(ب) $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ لكل $a,b,c \in R$.

(ج) $a\cdot(b+c) = a\cdot b + a\cdot c$ ، $(b+c)\cdot a = b\cdot a + c\cdot a$ لكل $a,b,c \in R$.

ويقال عن حلقة $(R,+,\cdot)$ أنها إبدالية ، إذا كان $a\cdot b = b\cdot a$ لكل $a \in R$
ويقال عن حلقة $(R,+,\cdot)$ أنها ذات عنصر محايد إذا وجد $1 \in R$ بحيث أن $a\cdot 1 = 1\cdot a = a$ لكل $a \in R$.

مثال (٢) :

(أ) كل من $(Z,+,\cdot)$ ، $(R,+,\cdot)$ ، $(Q,+,\cdot)$ حلقة إبدالية ذات عنصر محايد .

(ب) إذا كانت $R = (Z_n, \oplus, \odot)$ ، $Z_n = \{0,1,2,\cdots,n-1\}$ ، $a \oplus b = (a+b) \bmod n$ ، $a \odot b = (a.b) \bmod n$ ، فإن R حلقة إبدالية ذات عنصر محايد .

(ج) إذا كان $Z(i) = \{a+bi \mid a,b \in Z , i^2 = -1\}$ حيث لكل $x = a+bi \in R$ ، $y = c+di$ ، $x+y = (a+c)+(b+d)i$ ، $xy = (ac-bd)+(ad+bc)i$ ، فإن R حلقة إبدالية ذات عنصر محايد . تسمى $Z(i)$ أعداد جاوس (Gaussian integers) .

تعريف ٧-٣-٣ :

إذا كان R حلقة ، فيقال عن $0 \neq a \in R$ أنه قاسم صفري (Zero divisor) إذا وجد $0 \neq b \in R$ بحيث أن $ab = ba = 0$.

مثال (٣) :

(أ) إذا كانت $R = (Z_6, \oplus, \odot)$ ، فإن كلاً من 2,3,4 قاسم صفري ، لأن $2\odot 3 = 3\odot 2 = 0$ ، $4\odot 3 = 3\odot 4 = 0$.

(ب) كل من الحلقات $(Z_3, \oplus, \odot)$ ، $(Z,\oplus,\cdot)$ ، $(Q,+,\cdot)$ ، $(R,+,\cdot)$ ، $(Z(i),+,\cdot)$ ، لا تحوي قواسم صفرية .

تعريف ٧-٣-٤ :

يقال عن حلقة إبدالية ذات عنصر محايد أنها منطقة صحيحة Integral domain ، إذا كانت خالية من القواسم الصفرية .

مثال (٤) :

(أ) كل من $(Z,+,\cdot)$ ، $(Q,+,\cdot)$ ، $(R,+,\cdot)$ ، $(Z(i),+,\cdot)$ ، $(C,+,\cdot)$ ، $(Z_p,\oplus,\odot)$ حيث p عدد أولي منطقة صحيحة .

(ب) $R = \left(Z(\sqrt{-3}) = \{a + b\sqrt{-3} \mid a, b \in Z\} , +, \cdot \right)$ حيث لكل $x = a + b\sqrt{-3}$ ، $y = c + d\sqrt{-3}$ ، $x + y = (a+c) + (b+d)\sqrt{-3}$ ، $xy = (ac - 3d) + (ad + bc)\sqrt{-3}$ منطقة صحيحة .

تعريف ٧-٣-٥ :

يقال عن منطقة صحيحة F أنها حقل (Field) ، إذا كان لكل عنصر غير صفري معكوس ضربي . لاحظ أن

$(F,+,\cdot)$حقل إذاً إذا فقط كان $(F,+)$ زمره إبدالية و $(F,*,\cdot)$ زمره إبدالية والضرب توزيعي على الجمع .

مثال (٥) :

(أ) كل من $(Z_p,\oplus,\odot)$ حيث p عدد أولي ، $(Q,+,\cdot)$ ، $(R,+,\cdot)$، $(C,+,\cdot)$ حقل .

(ب) إذا كان p عدداً أولياً ، فإن

$$F = \left(Q(\sqrt{p}) = \{a + b\sqrt{p} \mid a, b \in Q\} , +, \cdot \right)$$

حيث لكل $x = a + b\sqrt{p} \in F$ ، $y = c + d\sqrt{p}$ ،

$x + y = (a + c) + (b + d)\sqrt{p}$ ، $xy = (ac + bd\,p) + (ad + bc)\sqrt{p}$

حقل بينما $(Z(\sqrt{p}),+,\cdot)$ ليس حقلاً .

(ج) $F_1 = (Q(i) = \{a + bi | a, b \in Q\}, +, \cdot)$ حقـــل ، كمـــا أن $F_2 = (Q\sqrt{-3} = \{a + b\sqrt{-3} | a, b \in Q\}, +, \cdot)$ ، حيـــث لكـــل $x = a + b\sqrt{-3} \in F_2$ ، $y = c + d\sqrt{-3}$ ، $x + y = (a + c) + (b + d)\sqrt{-3}$
$xy = (ac - 3bd) + (ad + bc)\sqrt{-3}$ حقل .

<u>تعريف ٧-٣-٦ :</u>

يقال عن $r \in C$ أنه عدد جبري (Algebraic Number) إذا كـان r جـذراً لكثيرة حدود $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in Z[x]$.
وإذا كان $a_0 = 1$ يسمى r عدداً صحيحاً جبرياً (Algebraic integer) .

<u>مثال (٦) :</u>

(أ) أي عدد نسبي هو عدد جبري ، لأنه إذا كان $r = \frac{a}{b} \in Q$ ، فإن r جـذر لكثيرة الحدود $f(x) = bx - a \in Z[x]$.

(ب) إذا كان $r \in Z$ ، فإن r عدد صحيح جبري ، لأن r جذر لكثيرة الحـدود $f(x) = x - r \in Z[x]$. وتسمى Z مجموعة الأعداد الصحيحة الجبرية النسبية (Rational integers) .

(ج) $r = i \in C$ عـدد صـحيح جبـري ، لأن i جـذر لكثيـرة الحـدود $f(x) = x^2 + 1 \in Z[x]$.

(د) $r = \frac{1 + \sqrt{3}i}{2} \in C$ عدد صحيح جبري ، لأن r جـذر لكثيـرة الحـدود $f(x) = x^2 - x + 1 \in Z[x]$.

(هـ) $r = \frac{i}{2} \in C$ عدد جبري لكنه ليس عدداً صحيحاً جبريـاً ، لأن r جـذر لكثيرة الحدود $f(x) = 4x^2 + 1 \in Z[x]$.

ملاحظة :

أن مجموعة الأعداد الجبرية مع عمليتي الجمع والضرب تكّون حقلاً أما مجموعة الأعداد الصحيحة الجبرية مع عمليتي الجمع والضرب تكّون حلقه .

تعريف ٧-٣-٧ :

إذا كان m صحيحاً ليس مربعاً كاملاً ، وكان $Q(\sqrt{m}) = (\{a + b\sqrt{m} \mid a, b \in Q\} , +, \cdot)$، $x = a + b\sqrt{m} \in Q(\sqrt{m})$ فيعرف مقياس x (Norm) والذي يرمز له بالرمز $N(x)$ كالآتي :

$$N(x) = x\bar{x} = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2$$

مثال (٧) :

(أ) ليكن $F = (Q(i), +, \cdot)$ ، $x = a + ib \in F$. إذاً $N(x) = a^2 + b^2$.

(ب) $F = (Q(\sqrt{2}), +, \cdot)$ ، $x = a + b\sqrt{2}$ ، فإن $N(x) = a^2 - 2b^2$.

(ج) $F = (Q(\sqrt{-3}), +, \cdot)$ ، $x = a + b\sqrt{-3}$ ، فإن $N(x) = a^2 + 3b^2$.

تعريف ٧-٣-٨ :

يقال عن عدد صحيح جبري $r \in Q(\sqrt{m})$ أنه قابل للإنعكاس (invertible or uint) ، إذا كان $\frac{1}{r}$ عدداً صحيحاً جبرياً .

إذاً $r \in Q(\sqrt{m})$ قابل للإنعكاس إذاً وإذا فقط كان $N(r) = \mp 1$ وسنرمز لمجموعة العناصر القابلة للإنعكاس في $Q(\sqrt{m})$ بالرمز $R^{\times}$.

مثال (٨) :

(أ) إذا كان $F = (Q(i), +, \cdot)$ ، فإن $R^{\times} = \{-1, 1, i, -i\}$.

(ب) إذا كان $F = (Q(\sqrt{2}), +, \cdot)$ ، فإن $R^{\times} = \{(\sqrt{2} + 1)^n \mid n \in Z)$.

(ج) إذا كان $F = (Q(\sqrt{-3}), +, \cdot)$، فإن $R^{\times} = \{\mp 1, \frac{1 \mp \sqrt{3}i}{2}, \frac{-1 \mp \sqrt{3}i}{2}\}$.

تعريف ٧-٣-٩ :

يقال عن عنصرين $a,b\in R$ أنهما مترادفان أو متصاحبيان أو متشاركان (Assoiated elements)إذا كان $a = bu$ ، حيث u عنصر قابل للإنعكاس في R

مثال (٩) :

(أ) إذا كان $F=(Z,+,\cdot)$ ، $a\in R$ فإن $\mp a$ يرادف a ، لأن $R^{\times}=\{-1,1\}$ و $a=a\cdot 1$ أو $a=(-a)(-1)$.

(ب) إذا كانت $F=(Q(i),+,\cdot)$ ، فإن $R^{\times}=\{-1,1,i,-i\}$ ، وعليه فإن $a+bi$ ، $-a-bi$ ، $-b+ai$ ، $b-ai$ عناصر مترادفة .

(ج) إذا كانت $F=Q(\sqrt{-3}),+,\cdot)$ ، فإن $\theta=\sqrt{-3}$ تصاحب $\mp(1-w)\,,\mp(1-w^2)\,,\mp(w-w^2)=\mp\sqrt{-3}$ ، حيث $w=\dfrac{1+\sqrt{-3}}{2}$.

تعريف ٧-٣-١٠ :

إذا كانت R حلقة فيقال عن $\rho\in R$ أنه عنصر أولي (Prime element)، إذا كان

(أ) $\rho\neq 0$ ، ρغير قابل للإنعكاس .

(ب) إذا كان $\rho\setminus ab$ ، فإن $\rho\setminus a$ أو $\rho\setminus b$.

ملاحظة : إذا كان $N(\rho)=\mp p$ ، p عدد أولي ، فإن ρ عنصر أولي .

مثال (١٠) :

(أ) $\sqrt{-3}\in Q(\sqrt{-3})$ عدد صحيح جبري و $\sqrt{-3}$ عنصر أولي ، لأن $N(-3)=3$ عدد أولي بينما $2\in Q(\sqrt{-3})$ ليس عدداً أولياً ، لأن $N(2)=4$ عدد غير أولي .

والآن إلى المبرهنات الآتية ، والتي فيها $\theta=\sqrt{-3}$.

مبرهنة ٧-٣-٣:

إذا كانت $x \in Q(\sqrt{-3})$ عدداً صحيحاً جبرياً ، فإن $x \equiv 0 \bmod (\theta)$ أو $x \equiv 1 \bmod (\theta)$ أو $x \equiv -1 \bmod (\theta)$.

البرهان:

بما أن $x = \dfrac{a + b\theta}{2}$ ، حيث $a, b \in Z$ ، وكل من a, b عدد زوجي أو كل من a, b عدد فردي . إذاً

$$\frac{a + b\theta}{2} = \frac{(b + a\theta)\theta}{2} + 2a \equiv 2a (\bmod\ \theta)$$

لكن $2a \equiv 0, 1, -1 \ (\bmod\ 3)$ و $\theta \setminus 3$. إذاً $x \equiv 0, 1, -1 (\bmod\ \theta)$.

□

مبرهنة ٧-٣-٤:

ليكن كلاً من $x, y \in Q(\sqrt{-3})$ عدداً جبرياً لا يقبل القسمة على θ .

(أ) إذا كان $x \equiv 1 (\bmod\ \theta)$ ، فإن $x^3 \equiv 1 (\bmod\ \theta^4)$.

(ب) إذا كان $x \equiv -1 (\bmod\ \theta)$ ، فإن $x^3 \equiv -1 (\bmod\ \theta^4)$.

(ج) إذا كان $x^3 + y^3 \equiv 0 \ (\bmod\ \theta)$ ، فإن $x^3 + y^3 \equiv 0 \ (\bmod\ \theta^4)$.

(د) إذا كان $x^3 - y^3 \equiv 0 \ (\bmod\ \theta)$ ، فإن $x^3 - y^3 \equiv 0 \ (\bmod\ \theta^4)$.

البرهان:

بما أن $x \equiv \mp 1 (\bmod\ \theta)$ حسب مبرهنة (٧-٣-٣) . إذاً

(أ) إذا كان $x \equiv 1 (\bmod\ \theta)$ ، فإن $x = 1 + b\theta$ ، $b \in Z$ ، وعليه فإن

$$x^3 = (1 + b\theta)^3 = 1 + 3b\theta - 9b^2 + b^3\theta^3$$
$$\equiv 1 + 3b\theta + b^3\theta^3 (\bmod\ \theta^4)$$

لكن $\theta \setminus b(b-1)(b+1)$ حسب مبرهنة (٧-٣-٣) . إذاً $x^3 \equiv 1 (\bmod\ \theta^4)$.

(ب) إذا كان $x \equiv -1 (\bmod \theta)$ ، فإن $-x \equiv 1 (\bmod \theta)$ ، وعليه فإن $(-x)^3 \equiv 1 (\bmod \theta^4)$ ، وبالتالي فإن $x^3 \equiv -1 (\bmod \theta^4)$.

(ج) بما أن $\theta \setminus x(x-1)(x+1)$. إذاً $x^3 \equiv x (\bmod \theta)$ ، وعليه فإن $x^3 + y^3 \equiv 0 \ (\bmod \theta)$ يعني أن $x + y \equiv 0 \ (\bmod \theta)$. فإذا كان $x \equiv 1 (\bmod \theta)$ ، فإن $y \equiv -1 (\bmod \theta)$ ، وعليه فإن $x^3 + y^3 \equiv 0 \ (\bmod \theta^4)$.

(د) إذا كان $x^3 - y^3 \equiv 0 \ (\bmod \theta)$ ، فإن $x^3 + (-y)^3 \equiv 0 \ (\bmod \theta)$ ، وعليه فإن $x^3 + (-y)^3 \equiv 0 \ (\bmod \theta^4)$ ومنها نجد أن $x^3 - y^3 \equiv 0 \ (\bmod \theta^4)$.

□

مبرهنة ٧-٣-٥:

لتكن $a, b, c \in \mathbb{Q}(\sqrt{-3})$ أعداداً صحيحة جبرية ، $a^3 + b^3 + c^3 = 0$. إذا كان $(a, b, c) = 1$ ، فإن واحدا فقط من الأعداد a, b, c يقبل القسمة على θ .

البرهان :

نفرض أن كلاً من a, b, c لا يقبل القسمة على θ . إذاً $0 = a^3 + b^3 + c^3 = \mp 1 \mp 1 \mp 1 \ (\bmod \theta^4)$ حسب مبرهنة (٧-٣-٤) . وعليه فإن θ^4 قاسم إلى $-1, 1, 3$ أو -3 . لكن $\theta^4 = 9$. إذاً واحد على الأقل من a, b, c يقبل القسمة على θ .

وإذا فرضنا أن أثنين من a, b, c يقبل القسمة على θ ، فإن ذلك يعني أن العدد الثالث يقبل القسمة على θ ، وبالتالي فإن $(a, b, c) \neq 1$ ، وهذا خلاف الفرض. إذاً واحد فقط من الأعداد a, b, c يقبل القسمة على θ .

□

مبرهنة ٧-٣-٦:

لتكن $a,b,c \in Q(\sqrt{-3})$ أعداد صحيحة جبرية ، $\theta \nmid abc$ وليكن $\alpha,\beta \in Q(\sqrt{-3})$ عنصرين قابلين للإنعكاس ، $n \in Z^+$ ، $a^3+\alpha b^3+\beta(\theta^n c)^3=0$ ، فإن $\alpha=\mp 1$, $n \geq 2$.

البرهان :

بما أن $n>2$. إذاً $a^3+\alpha b^3 \equiv 0 (\bmod\ \theta^3)$ ، وعليه فإن $a^3+\alpha b^3 \equiv \mp 1+\alpha(\mp 1) \equiv 0 (\bmod\ \theta^3)$ حسب مبرهنة (٧-٣-٤) . لكن $\alpha \in \{\mp 1, \mp w, \mp w^2 | w=\frac{-1+\sqrt{-3}}{2}\}$. إذاً

$$\mp 1+\alpha(\mp 1) \in S=\{-2,0,2,\mp(1\mp w),\mp(1\mp w^2)\}$$

لكن θ^3 لا تقسم أياً من عناصر S ما عدا الصفر ، لأن $(1-w^2)$ ، $(1-w)$ ترادف θ و $1+w=-w^2$ و $1+w^2=-w$ عناصر قابلة للإنعكاس و $N(\mp 2)=4$ بينما $N(\theta^3)=27$. إذاً $\mp 1+\alpha(\mp 1)=0$ ، وعليه فإن $\alpha=\mp 1$. لكن $a^3+\alpha b^3 \equiv 0 (\bmod\ \theta^3)$ يعني أن $a^3+\alpha b^3 \equiv 0 (\bmod\ \theta^4)$ ، وعليه فإن $\theta^4 \setminus \beta(\theta^n c)^3$ ومنها نجد أن $n \geq 2$.

□

مبرهنة ٧-٣-٧:

لا توجد $a,b,c \in Q(\sqrt{-3})$ وعنصر قابل للإنعكاس $\alpha \in Q(\sqrt{-3})$ و $n \geq 2$ بحيث أن

$$a^3+b^3+\alpha(\theta^n c)^3=0 \qquad \dots (1)$$

البرهان :

يمكن أن نفرض أن $(a,b,\theta^n c)=1$ و $\theta \nmid c$ ، θ لا تقسم a,b معاً ، لذا يمكن أن نفرض أن $\theta \nmid b$.

والآن لنفرض وجود أعداد صحيحة تحقق المعادلة (1) وأن S هي مجموعة تلك الأعداد . وحيث أن $N(x)>0$ لكل $x \in Q(\sqrt{-3})$ ، $N(\alpha)=1$. إذاً يمكننا أن نختار مجموعة T بحيث أن

$$T=\{a,b,c \in S \mid \text{أقل ما يمكن } N(a^3b^3\theta^{3n}c^3)\}$$

لكن $n \geq 2$. إذاً $a^3+b^3 \equiv 0 \pmod{\theta^6}$ ، كما أن

$$w=\frac{-1+\sqrt{-3}}{2} \text{ ، } a^3+b^3=(a+b)(a+wb)(a+w^2b) \quad \ldots (2)$$

سنبرهن على أن أي عدد أولي p يقسم أي أثنين من $a+b, a+bw, a+bw^2$ يرادف θ . ولإثبات ذلك لاحظ أن إذا كان $p \backslash (a+b)$ و $p \backslash (a+bw)$ ، فإن $p \backslash b(1-w)$ و $p \backslash a(1-w)$ ، لكن $(a,b)=1$ و $(1-w)$ يرادف θ .

وإذا كان $p \backslash (a+b)$ و $p \backslash (a+bw^2)$ ، فإن $p \backslash (1-w^2)b$ و $p \backslash (1-w^2)a$ ، وعليه فإن $p \backslash (1-w^2)$ ، وبالتالي فإن $p \backslash \theta$.

أما إذا كان $p \backslash (a+bw)$ و $p \backslash (a+bw^2)$ ، فإن $p \backslash (w-w^2)b$ و $p \backslash (w-w^2)a$ ، وعليه فإن $p \backslash \theta$. وبما أن $\theta \nmid b$ و

$$\theta \text{ ترادف } \mp(1-w), \mp(1-w^2), \mp(w-w^2)=\mp\theta \quad \ldots (3)$$

إذاً الفروق بين $a+b, a+bw, a+w^2$ تقبل القسمة على θ لكنها لا تقبل القمسة على θ^2 ، كما أن $\theta^6 \backslash (a+b)(a+bw)(a+bw^2)$.

وعليه إذا كان $\theta^r, \theta^s, \theta^t$ هي أكبر القوى للعدد θ التي تقسم $a+b, a+bw, a+bw^2$ على التوالي ، فإن (1) تعني أن $r,s,t \in \{1,1,3n-2\}$ و $\frac{a+b}{\theta^r}, \frac{a+bw}{\theta^s}, \frac{a+bw^2}{\theta^t}$ أعداد صحيحة في $Q(\sqrt{-3})$ لا يوجد بينها قاسم أولي وبتطبيق (3) ، نجد أن

$$\frac{a+b}{\theta^r}\cdot\frac{a+bw}{\theta^s}\cdot\frac{a+bw^2}{\theta^t}=-\alpha c^3 \quad \ldots (4)$$

وعليه فإن أي عامل من عوامل الطرف الأيسر في (4) يرادف مكعب عدد صحيح . إذاً

$$a+b=\alpha_1\theta^r\lambda_1^3\ ,\ a+bw=\alpha_2\theta^s\lambda_2^3,\ a+bw^2=\alpha_3\theta^t\lambda_3^3 \quad \dots (5)$$

حيث $\lambda_1,\lambda_2,\lambda_3$ عناصر قابلة للإنعكاس . لكن

$$(a+b)+w(a+bw)+w^2(a+bw^2)=(a+b)\,(1+w+w^2)=0$$

إذاً

$$\alpha_1\theta^r\lambda_1^3+\alpha_4\theta^s\lambda_2^2+\alpha_5\theta^t\lambda_3^3=0 \quad \dots (6)$$

حيث $\alpha_5=w^2\alpha_3\ ,\ \alpha_4=w\,\alpha_2$ ، وعليه فإن α_4,α_5 عناصر قابلة للإنعكاس ، وبالتالي يمكن أن تأخذ r,s,t القيم $1,1,3n-2$ بأي ترتيب كان لذلك يمكن أن نفرض أن $r=1,s=1,t=3n-2$. وبالتعويض في (6) والقسمة على $\alpha_1\theta$ نجد أن

$$\lambda_1^3+\alpha_6\lambda_2^3+\alpha_7(\theta^{n-1}\lambda_3)^3=0 \quad \dots (7)$$

حيث $\alpha_6=\dfrac{\alpha_4}{\alpha_1},\ \alpha_7=\dfrac{\alpha_5}{\alpha_1}$ عناصر قابلة للإنعكاس . لكن $c\neq 0$ ، إذاً $\lambda_1\lambda_2\lambda_3\neq 0$ ، كما أن $\theta\nmid\lambda_1\lambda_2\lambda_3$. إذاً $\alpha_6=\mp 1$ ، $(n-1)\geq 2$ حسب مبرهنة (٧-٣-٦) . لكن للمعادلة (7) نفس شكل المعادلة (1) ، لأن

$$\alpha_6\lambda_2^3=(-\lambda_2)^3 \text{ أو } \alpha_6\lambda_2^3=\lambda_2^3$$

وحيث أن $N(\theta)=3$ ، $N(a)\geq 1$ ، $N(b)\geq 1$. إذاً من (4) ، (5) نجد أن $r+s+t=3n$ و

$$N(\lambda_1^3\ \lambda_2^3\,\theta^{3n-3}\lambda_3^3)=N(\theta^{-3}(a+b)(a+bw)(a+bw^2))$$
$$=N(\theta^{3n-3}\cdot c^3)<N(a^3\,b^3\,\theta^{3n}\,c^3)$$

وهذا يناقض كون $N(a^3\,b^3\theta^{3n}\,c^3)$ أقل ما يمكن .

□

مبرهنة ٧-٣-٨:

لا توجد أعداد صحيحة غير صفرية $a,b,c \in Q(\sqrt{-3})$ بحيث أن $a^3+b^3+c^3=0$. ولا توجد أعداد صحيحة غير صفرية $x,y,z \in Q(\sqrt{-3})$ بحيث أن $x^3+y^3=z^3$.

البرهان :

نفرض وجود أعداد صحيحة $a,b,c \in Q(\sqrt{-3})$ ، بحيث أن $a^3+b^3+c^3=0$ ، ولنفرض أن $(a,b,c)=1$. إذاً بتطبيق مبرهنة (٧-٣-٥) ، نجد أن واحداً فقط من الأعداد a,b,c يقبل القسمة على θ ، ولنفرض أنه c ، كما أن θ^n هي أكبر قوة للعدد θ بحيث أن $\theta^n \setminus c$. إذاً $c=\theta^n \cdot r$ و $\theta \nmid r$ ، لكن $n \geq 2$ حسب مبرهنة (٧-٣-٦) و $(a^3+b^3+(0^3 r)^3=0$ وهذا يناقض مبرهنة (٧-٣-٧). إذاً لا توجد أعداد صحيحة غير صفرية a,b,c بحيث أن $a^3+b^3+c^3=0$. لكن $x^3+y^3=z^3 \Leftrightarrow x^3+y^3+(-z)^2=0$. إذاً لا توجد أعداد صحيحة غير x,y,z بحيث أن $x^3+y^3=z^3$.

□

تمارين

(١) برهن على عدم وجود حل في Z لكل من المعادلات الآتية :

(أ) $x^4+2y^4=z^2$ ، (ب) $x^4+4y^4=z^2$

(ج) $x^4-y^4=2z^2$ ، (د) $x^4-4y^4=z^2$

(٢) برهن على وجود عدد غير منتهي من الحلول في Z للمعادلة $x^4+y^4=2z^2$.

(٣) برهن على عدم وجود حل في Z ، للنظام
(أ) $x^2+y^2=z^2$ و $x^2-y^2=w^2$ ، (ب) $x^2+y^2=z^2, x^2+2y^2=w^2$

(٤) برهن على وجود عدد غير منتهي من الحلول في Z ، للنظام $x^2+y^2=z^2+1$ و $x^2-y^2=w^2+1$.

٧-٤ : مجموع مربعين أو أكثر Sum of two or more than two squares

بدأت دراسة مسألة تحليل عدد طبيعي إلى مجموع مربعات أعداد طبيعية من قبل ديوفنتس ، وطورت من قبل الرياضيين العرب في القرن العاشر للميلاد .

ودُرس تمثيل الأعداد الأولية على شكل مجموع مربعات من قبل الفرنسيان باشيه وفيرما . وسنركز اهتمامنا في هذا الجزء على أثبات بعض قضايا الخازن ومبرهنة جيرارد – فيرما " يمكن التعبير عن عدد أولي فردي p كمجموع مربعين إذاً وإذا فقط كان $p \equiv 1 \pmod 4$ " ، ثم نثبت أنه إذا كان $n = k^n m$ عدد صحيحاً موجباً وكان m ليس مربعاً ، فيمكن التعبير عن n كمجموع مربعين إذاً وإذا فقط كانت جميع القواسم الأولية للعدد m ليست على الشكل $4t+3$ ، ثم ندرس كيفية التعبير عن عدد طبيعي كمجموع أربعة مربعات والتي بدأت دون إثبات مع باشيه ، ثم أثبتت من قبل لاجرانج وأويلر.

ونبدأ بالقضية الآتية والتي أثبت من قبل أبو جعفر الخازن في القرن العاشر للميلاد .

قضية ٧-٤-١: " الخازن "

إذا كان $m = a^2 + b^2$ ، $n = c^2 + d^2$ عددين طبيعيين ، فيمكن التعبير عن $m\,n$ كمجموع مربعين بشكلين مختلفين .

البرهان :

بما أن $m = a^2 + b^2$ و $n = c^2 + d^2$. إذاً

$$mn = (a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ab-bc)^2$$
$$= (ac-bd)^2 + (ad+bc)^2$$

□

مثال(١) :

(أ) بما أن $5 = 2^2 + 1^2$ ، $13 = 2^2 + 3^2$. إذاً

$$65 = 5 \cdot 13 = (4+3)^2 + (6-2)^2 = 7^2 + 4^2$$
$$= (4-3)^2 + (6-2)^2 = 1^2 + 8^2$$

(ب) بما أن $17 = 4^2 + 1^2$ ، $29 = 5^2 + 2^2$. إذاً

$$493 = 7 \cdot 29 = (4^2 + 1^2)(5^2 + 2^2) = (20+2)^2 + (8-5)^2 = (22)^2 + 3^2$$
$$= (20-2)^2 + (8+5)^2 = (18)^2 + (13)^2$$

والآن إلى القضية الآتية التي تعود إلى النوريجي ثو "١٨٦٣-١٩٢٢،Thue " .

مبرهنة ٧-٤-٢:

إذا كان p عدداً أولياً ، $a \in Z$ ، $(a,p) = 1$ ، فإن للتطابق الخطي $ax \equiv y \pmod p$ حل $x = b , y = c$ و $0 < |b| < \sqrt{p}$ ، $0 < |c| < \sqrt{p}$.

البرهان :

ليكن $k = [\sqrt{p}] + 1$ ، ولتكن $S = \{ax - b | 0 \le x \le k-1 , 0 \le y \le k-1\}$
إذاً $|S| = k^2 > p$ ، وعليه يوجد على الأقل عنصرين $ax_1 - y_1 , ax_2 - y_2 \in S$ ،
$x_1 \neq x_2$ ، $y_1 \neq y_2$ ، $ax_1 - y_1 \equiv ax_2 - y_2 \pmod p$ حسب قاعدة ديركلي
" إذا وضع n من الأشياء في m من الصناديق وكان $n > m$ ، فإن أحد الصناديق يحوي على الأقل على شيئين منها " . إذاً $a(x_1 - x_2) \equiv y_1 - y_2 \pmod p$ ،
وعليه فإن $b = x_1 - x_2$ ، $c = y_1 - y_2$ حل للتطابق $ax \equiv y \pmod p$.

وإذا كان $c = 0$ ، فإن $(a,p) = 1$ ، $ab \equiv c \pmod p$ يعني أن $b = 0$.
وإذا كان $b = 0$ ، فإن $(a,p) = 1$ يعني أن $c = 0$ وكلتا الحالتين تناقض كون $S \neq \{0\}$. إذاً $0 < |b| \le (k-1) < \sqrt{p}$ ، $0 < |c| \le (k-1) < \sqrt{p}$.

□

والآن إلى المبرهنة الآتية التي تعود إلى كل من جيراد (١٥٩٥-١٦٣٢م) وفيرما والتي أثبتت من قبل أويلر سنة ١٧٥٤م .

مبرهنة ٧-٤-٣: " جيراد – فيرما "

يمكن التعبير عن أي عدد أولي فردي p كمجموع مربعين إذاً وإذا فقط كان $p \equiv 1 \pmod p$.

البرهان: " أويلر "

نفرض أن $p = a^2 + b^2$. إذاً $p \equiv a^2 + b^2 (\text{mod } 4)$. لكـن $k^2 \equiv 0 \vee 1$ لكل $k \equiv 0,1,2,3 \ (\text{mod } 4)$. إذاً $a^2 , b^2 \equiv 0 \vee 1 (\text{mod } 4)$. لكـن p عـدد فردي إذاً أما

$(a^2 \equiv 0 \text{ mod } 4 \ \wedge \ b^2 \equiv 1 \text{ mod } 4)$ أو $(a^2 \equiv 1 \text{ mod } 4 \wedge b^2 \equiv 0 \text{ mod } 4)$،

وعليه فإن $p = (a^2 + b^2) \equiv 1 (\text{mod } 4)$.

ولإثبات العكس نفرض أن $p \equiv 1 (\text{mod } 4)$. إذاً $[(\frac{p-1}{2})!] + 1$ يقبل القـسمة على p ، وعليه فإن $[(\frac{p-1}{2})!]^2 \equiv -1 \ (\text{mod } p)$ ، وهذا يعنـي وجـود حـل للتطابق $a^2 \equiv -1 (\text{mod } p)$ ، وعليه فـإن $(-1)Rp$. لكـن $(a,p) = 1$. إذاً للتطابق $ax \equiv y \ (\text{mod } p)$ حل وليكن b,c و $0 < |b| < \sqrt{p}$ ، $0 < |c| < \sqrt{p}$ حسب قضية (٧-٤-٢) ، وعليه فإن $-b^2 \equiv a^2 b^2 = (ab)^2 \equiv c^2 (\text{mod } p)$ ، ومنها نجد أن $b^2 + c^2 = kp$ ، $1 \le k \in Z$. لكن

$$kp = b^2 + c^2 = |b|^2 + |c|^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = kp$$

إذاً $k < 2$. لكن $k \ge 1$. إذاً $k = 1$ ، وعليه فإن $p = b^2 + c^2$.

□

نتيجة :

إذا كان $p = 4m + 1$ عدداً أولياً ، فيمكن التعبيـر عـن p بطريقـة وحيـدة كمجموع مربعين .

البرهان :

نفـــــرض أن $p = a^2 + b^2 = c^2 + d^2$ ، حيـــــث $a,b,c \in Z^+$. إذاً $a^2 d^2 - b^2 c^2 = p\,(d^2 - b^2) \equiv 0 \ (\text{mod } p)$ ، وعليه فإن $ad \equiv bc \ \ (\text{mod } p)$ أو $ad \equiv -bc \ \ (\text{mod } p)$. لكـن كـلاً مـن a,b,c,d أقـل مـن $\sqrt{p}$. إذاً $ad - bc = 0$ أو $ad + bc = p$. فإذا كان $ad + bc = p$ ، فإن

$$p^2 = (a^2 + b^2)\,(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 = p^2 + (ac - bd)^2$$

وعليه فإن $ac - bd = 0$ ومنها نجد أن $ac = bd$ ، وبالتالي فــإن $ad = bc$ أو $ac = bd$. فإذا كان $ad = bc$ ، فإن $a \backslash bc$ و $(a,b) = 1$ يعنــي أن $a \backslash c$ ، وعليه فإن $c = ar$ حيث $r \in Z^+$ ، وبالتالي فإن $ad = bc = b(ar)$ ومنها نجد أن $d = br$. لكـــــن $p = c^2 + d^2 = r^2(a^2 + b^2)$ يعنـــــي أن $r = 1$. إذاً $a = c$ و $b = d$. وإذا كان $ac = bd$ فبنفس الطريقة يمكــن أن نثبــت أن $a = d$ ، $b = c$ ، وعليه يمكن كتابة p بطريقة وحيدة كمجموع مربعين .

□

مثال (٢) :

(أ) $17 \equiv 1 \pmod 4$ ، $17 = 4^2 + 1^2$.

(ب) $5 \equiv 1 \pmod 4$ ، $5 = 2^2 + 1^2$.

(ج) $29 \equiv 1 \pmod 4$ ، $29 = 5^2 + 2^2$.

(د) $113 \equiv 1 \pmod 4$ ، $113 = 7^2 + 8^2$.

(هـ) $3 \not\equiv 1 \pmod 4$ ، $3 \neq a^2 + b^2$ لكل $a,b \in Z$.

وبصورة عامة يمكن أن نبرهن ما يلي .

قضية ٧-٤-٤:

لا يمكن التعبير عن العدد الأولي $p = 4m + 3$ ، $m \in Z^+$ ، كمجموع مربعين.

البرهان :

بما أن $a \equiv 0,1,2,3 \pmod 4$ لكل $a \in Z$. إذاً $a^2 \equiv 0 \vee 1$ لكل $a \in Z$ ، وعليـــــه فــــإن $a^2 + b^2 \equiv 0,1,2 \pmod 4$. لكـــــن $p = 4m + 3$. إذاً $a^2 + b^2 \neq p$.

□

مثال (٣) :

عبر عن العدد 85 كمجموع مربعين بشكلين مختلفين .

الحل :

بما أن $85 = 5 \cdot 17$ ، وكل من $5,17$ أعداد أولية على الشكل $4m+1$. إذاً يمكن التعبير عن كل منها كمجموع مربعين حسب مبرهنة (٧-٤-٣) . وبإستخدام قضية (٧-٤-١) ، نجد أن

$$85 = 5 \cdot 17 = (2^2+1^2)\,(4^2+1^2) = (8+1)^2 + (2-4)^2 = 9^2 + 2^2$$

$$= (8-1)^2 + (2+4)^2 = 7^2 + 6^2$$

والآن إلى المبرهنة الآتية التي توضح متى يمكن التعبير عن عدد طبيعي كمجموع مربعين .

مبرهنة ٧-٤-٥:

إذا كان $n = k^2 m$ عدد صحيحاً موجباً وكان m ليس مربعاً ، فيمكن التعبير عن n كمجموع مربعين إذاً وإذا فقط كانت جميع القواسم الأولية للعدد m ليست على الشكل $4t+3$ ، $t \in Z^+$.

البرهان :

نفرض أن جميع القواسم الأولية للعدد m ليست على الشكل $4t+3$. فإذا كان $m=1$ ، فإن $n = k^2 + 0^2$ ويتم المطلوب . أما إذا كان $m>1$ ، فأفرض أن $m = \prod_{i=1}^{r} p_i$ حيث p_i أعداد أولية مختلفة ليست على الشكل $4t+3$. إذاً أما $p_i = 2$ لكل $i = 1,2,\cdots,r$ أو $p_i \equiv 1 (\text{mod } 4)$. فإذا كان $p_i = 2$ لكل i ، فإن $p_i = 1^2 + 1^2$ ، وإذا كان $p_i \equiv 1 (\text{mod } 4)$ لكل i فإن $p_i = a_i^2 + b_i^2$ حسب مبرهنة (٧-٤-٣) . لكن

$$p_1 p_2 = (a_1^2 + b_1^2)\,(a_2^2 + b_2^2) = (a_1a_2 + b_1b_2)^2 + (a_1a_2 - b_1a_2)^2$$

حسب قضية (٧-٤-١) . إذاً بالأستقراء على r يمكن أن نبرهن أن $m = \prod_{i=1}^{r} p_i = a^2 + b^2$. إذاً $n = k^2 m = k^2(a^2+b^2) = (ka)^2 + (kb)^2$

ولإثبات العكس نفرض أن $n = a^2 + b^2 = k^2 m$ ، p قاسم أولي للعدد m .

ولـــيكن $d=(a,b)$. إذاً $a=rd$ ، $b=sd$ ، $(r,s)=1$ ، وعليـــه فـــإن $n=d^2(r^2+s^2)=k^2m$. لكن m ليس مربعاً كاملاً ، $d^2 \backslash k^2$. إذاً

$$r^2+s^2=(\frac{k^2}{d^2})m=pu \text{ ، حيث } u\in Z .$$

وعليـــه فـــإن $r^2+s^2\equiv 0 \pmod p$. لكـــن $(r,s)=1$. إذاً $(r,p)=1$ أو $(s,p)=1$ ، وعليه يمكن أن نفرض $(r,p)=1$ ، إذاً يوجـد معكـوس ضـربي للعدد r وليكن v . إذاً $rv\equiv 1 \pmod p$. لكـــن $r^2+s^2\equiv 0 \pmod p$ ، إذاً $v^2(r^2+s^2)\equiv 0 \pmod p$ ، وعليه فإن $(rv)^2+(sv)^2\equiv 0 \pmod p$ ، ومنها نجـد أن $(sv)^2+1\equiv 0 \pmod p$ ، وعليـــه فـــإن $p\equiv 1 \pmod 4$ حـسب مبرهنة (٣-٦-٣) ، وهذا يعني عدم وجـود أي قاسـم أولـي إلـى m علـى الصورة $(4t+3)$.

□

مثال (٤) : أياً من الأعداد الآتية يمكن التعبير عنه كمجموع مربعين ؟
(أ) 425 ، (ب) 783 ، (ج) 2349 .

الحل :

(أ) بما أن $425=5^2\cdot 17$ ، $17\not\equiv 3 \pmod 4$ ، إذاً يمكن التعبير عـن 425 كمجموع مربعين . لاحظ أن

$$425=5^2\cdot 17=5^2(4^2+1^2)=(5\cdot 4)^2+(5)^2=(20)^2+5^2$$

(ب) بمـا أن $783=3^3\cdot 29=3^2\cdot(3\cdot 29)$ و $3\equiv 3 \pmod 4$ إذاً لا يمكـن التعبير عن 783 كمجموع مربعين .

(ج) $2349=3^4\cdot 29=(3^2)^2\cdot 29$ ، $29\equiv 1 \pmod 4$ ، إذاً يمكـن التعبيـر عن 2349 كمجموع مربعين . لاحظ أن

$$2349=(3^2)^2\cdot 29=(3^2)^2(5^2+2^2)=(3^2\cdot 5)^2+(3^2\cdot 2)^2$$
$$=(45)^2+(18)^2$$

والآن إلى المبرهنة الآتية التي أثبتت من قبل أبو جعفر الخازن في القرن العاشر للميلاد .

مبرهنة ٧-٤-٦: " الخازن "

(أ) إذا كتب عدد طبيعي كمجموع مربعين ، فإن مربعه يكتب أيضاً كمجموع مربعين .

(ب) إذا كتب عدد مربع كمجموع مربعين ، فإن مربعه يكتب بشكلين مختلفين كمجموع مربعين .

(ج) إذا أمكن التعبير عن عدد كمجموع مربعين ، فيمكن التعبير عن ضعفه كمجموع مربعين .

(د) إن حاصل ضرب عددين ينقسم أحدهما إلى مربعين بشكلين مختلفين ، وينقسم الآخر إلى مربعين بشكل وحيد ، ينقسم إلى مجموع مربعين بأربعة أشكال مختلفة .

البرهان :

(أ) نفرض أن $n = a^2 + b^2$. إذاً $n^2 = (a^2 + b^2)^2 = (a^2 - b^2)^2 + 4a^2b^2$.

(ب) نفرض أن $n^2 = a^2 + b^2$ ، حيث $n, a, b \in \mathbb{N}$ ، إذاً $n^4 = n^2 \cdot n^2 = n^2a^2 + n^2b^2 = (na)^2 + (nb)^2$ ، كما أن $n^4 = (a^2 + b^2)^2 = (a^2 - b^2)^2 + (2ab)^2$.

(ج) نفرض أن $n = a^2 + b^2$ ، $a \neq b$. إذاً $2n = (a + b)^2 + (a - b)^2$.

(د) نفرض أن $m = a^2 + b^2 = r^2 + s^2$ ، $n = c^2 + d^2$. إذاً

$$mn = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2$$
$$= (rc + sd)^2 + (rd - sc)^2 = (rd + sc)^2 + (rc + sd)^2$$

□

مثال (٥) :

(أ) $17 = 4^2 + 1^2$ ، $289 = (17)^2 = (4^2 - 1^2)^2 + (2 \cdot 4 \cdot 1) = (15)^2 + 8^2$ ، $(289)^2 = [(15)^2 - 8^2]^2 + (2 \cdot 15 \cdot 8)^2 = (161)^2 + (240)^2$.

(ب) $25 = 4^2 + 3^2$ ،

$626 = (25)^2 = 25(4^2 + 3^2) = (5\cdot 4)^2 + (5\cdot 3)^2 = (20)^2 + (15)^2$ ،

$625 = (25)^2 = (4^2 + 3^2)^2 = (4^2 - 3^2)^2 + (2\cdot 4\cdot 3)^2 = 7^2 + (24)^2$.

(ج) $29 = 5^2 + 2^2$ ، $58 = 2\cdot 29 = (5+2)^2 + (5-2)^2 = 7^2 + 3^2$ ،

$116 = 2(58) = (7+3)^2 + (7-3)^2 = (10)^2 + 4^2$ ،

$232 = 2(116) = (10+4)^2 + (1-4)^2 = (14)^2 + 6^2$.

(د) $m = 65 = 7^2 + 4^2 = 8^2 + 1^2 \quad , \quad n = 17 = 4^2 + 1^2$

$$mn = (65)(17) = 1105 = (7\cdot 4 + 4\cdot 1)^2 + (7\cdot 1 - 4\cdot 4)^2 = (32)^2 + 9^2$$

$$= (7+16)^2 + (7\cdot 4 - 4\cdot 1)^2 = (23)^2 + (24)^2$$

$$= (8\cdot 4 + 1\cdot 1)^2 + (8\cdot 1 - 1\cdot 4)^2 = (33)^2 + 4^2$$

$$= (8+4)^2 + (32-1)^2 = (12)^2 + (31)^2$$

والآن إلى دراسة كيفية التعبير عن عدد صحيح موجب كمجموع أربعة مربعات والتي بدأت دون إثبات مع الفرنسي باشيه سنة ١٦٢١م ، ثم أثبتت من قبل لاجرانج سنة ١٧٧٢م وأويلر سنة ١٧٧٣م ويعتمد البرهان على القضية الآتية .

قضية ٧-٤-٧: " أويلر "

إذا أمكن التعبير عن كل من m, n كمجموع أربعة مربعات ، فإنه يمكن التعبير عن $m\,n$ كمجموع أربعة مربعات .

البرهان :

نفرض أن $m = \sum_{i=1}^{4} a_i^2$ ، $n = \sum_{i=1}^{4} b_i^2$. إذاً

$$mn = (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2$$
$$+ (a_1b_3 - a_2b_4 - a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 - a_4b_1)^2$$

□

مثال (٦) :

إذا كان $m = 154$ ، $n = 39$ ، فإن

$$m = 8^2 + 7^2 + 5^2 + 4^2 \ , \ n = 5^2 + 3^2 + 2^2 + 1^2$$ ،

$$mn = (40+21+10+4)^2 + (24-35+5-8)^2 + (16-7-25+12)^2$$
$$+ (8+14-15-20)^2 = (75)^2 + (14)^2 + 4^2 + (13)^2$$

مبرهنة ٧-٤-٨:

إذا كان p عدداً أولياً فردياً ، فيوجد $m \in Z$ ، $1 \le m < p$

بحيث أن $mp = \sum_{i=1}^{4} x_i^2$ ، $x_i \in Z$.

البرهان :

بما أن p عدد أولـــي فـــردي . إذاً $p \equiv 1 \ (\text{mod } 4)$ أو $p \equiv 3 \ (\text{mod } 4)$.

فإذا كان $p \equiv 1 \ (\text{mod } 4)$ ، فإن للتطـــابق $x^2 \equiv -1 \ (\text{mod } p)$ حـــل حـــسب مبرهنة (٣-٦-٣) ، وعليه إذا كـــان x_1 حـــلاً للتطـــابق $x^2 \equiv -1 \ (\text{mod } p)$ وكان $y_1 = 0$ ، فإن $x_1^2 + y_1^2 + 1 \equiv 0 (\text{mod } p)$ ، وعليه فإن

$$mp = x_1^2 + y_1^2 + 1^2 + 0^2 \ ، \ 0 < x_1 \le \frac{p-1}{2} \ .$$

أما إذا كان $p \equiv 3 \ (\text{mod } 4)$ ، فأفرض أن a أصغر باقي موجب غير تربيعـــي قياس p . إذاً $(-a/p) = (-1/p)(a/p) = (-1)(-1) = 1$ حسب تعريف رمـــز لجندر ونتيجة مبرهنة (٦-٢-٢) ، وعليه فإن $(-a)Rp$ ، وهذا يعني أن للتطابق $x^2 \equiv -a \ (\text{mod } p)$ حـــل ولـــيكن x_1 ، $0 < x_1 \le \frac{p-1}{2}$ ، وحيـــث أن $0 < a - 1 < a$. إذاً $(a-1)Rp$ ، وعليه يوجد $y_1 \in Z^+$ ، $0 < y_1 \le \frac{p-1}{2}$ بحيث أن $y_1^2 \equiv a - 1 (\text{mod } p)$. إذاً $x_1^2 + y_1^2 + 1 \equiv 0 (\text{mod } p)$ ، وعليه فإن $mp = x_1^2 + y_1^2 + 1^2 + 0^2$ ، كما أن

$$1 \le m = \frac{1}{p}(x_1^2 + y_1^2 + 1) \le \frac{1}{p}[2(\frac{p-1}{2})^2 + 1] < \frac{1}{p} \cdot (\frac{p^2}{2} + 1) < p \ .$$

□

مبرهنة ٧-٤-٩:

يمكن التعبير عن أي عدد أولي كمجموع أربعة مربعات .

البرهان :

إذا كان $p = 2$ ، فإن $2 = 1^2 + 1^2 + 0^2 + 0^2$ ، أما إذا كان p عدداً فردياً ، فأفرض أن m هو أصغر عدد صحيح موجب يحقق العلاقة

$$m < p \text{ ، } mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \quad \ldots (1)$$

سنثبت أن $m = 1$ ، ولإثبات ذلك نفرض أن $m > 1$. إذاً أما m عد زوجي أو m عدد فردي . فإذا كان m عدداً زوجياً فإن mp عدد زوجي وعليه إما x_i زوجية لكل $i = 1, 2, 3, 4$ أو أن x_i فردين لكل $i = 1, 2, 3, 4$ أو أن أثنين منها زوجية والآخرى فردية ، وفي جميع الحالات نجد أن $x_1 \mp x_2 \ , x_3 \mp x_4$ عددان زوجيان ، وعليه فإن

$$(\frac{m}{2})p = (\frac{x_1 + x_2}{2})^2 + (\frac{x_1 - x_2}{2})^2 + (\frac{x_3 + x_4}{2})^2 + (\frac{x_3 - x_4}{2})^2 \text{ ،}$$

$0 < \frac{m}{2} < m$ وهذا يناقض كون m أصغر عدد صحيح موجب يحقق العلاقة (1) .

وإذا كان m عدداً فردياً ، فإن $3 \le m < p$. ولنعرّف $y_i \equiv x_i \pmod m$ ، $-(\frac{m-1}{2}) \le y_i \le \frac{m-1}{2}$ ، $i = 1, 2, 3, 4$ ، $\sum_{i=1}^{4} y_i^2 \equiv \sum_{i=1}^{4} x_i^2 \pmod m$.

لكن $\sum_{i=1}^{4} x_i^2 \equiv 0 \pmod m$ ، إذاً $\sum_{i=1}^{4} y_i^2 \equiv 0 \pmod m$ ، وعليه فإن $\sum_{i=1}^{4} y_i^2 = mn$ ، $0 \le n \le \frac{4}{m}(\frac{m-1}{2})^2 < m$. فإذا كان $n = 0$ ، فإن $y_i = 0$ لكل i ، وعليه فإن $x_i \equiv 0$ لكل i ، وبالتالي فإن $mp = \sum_{i=1}^{4} x_i^2 \equiv 0 \pmod{m^2}$ ، ومنها نجد أن $p \equiv 0 (\text{mod} \quad)$ وهذا غير ممكن لأن $3 \le m < p$. إذاً $n > 0$ ، وعليه فإن

$m^2np = (\sum_{i=1}^{4} x_i^2)(\sum_{i=1}^{4} y_i^2) = \sum_{i=1}^{4} a_i^2$ حسب قضية (٧-٤-٧) . وبالتالي فإن $np = \sum_{i=1}^{4} (\frac{a_i}{m})^2$ و $0 < n < m$ ، وهذا يناقض كون m أصغر عدد صحيح موجب يحقق العلاقة (1) . إذاً $m = 1$.

□

<u>مبرهنة ٧-٤-١٠:</u> " باشية – لارانج "

يمكن كتابة أي عدد صحيح موجب كمجموع أربعة مربعات .

<u>البرهان :</u>

نفرض أن n عدد صحيح موجب . إذاً إذا كان $n = 1$ ، فإن $1 = 1^2 + 0^2 + 0^2 + 0^2$. وإذا كان $n > 1$ ، فلنفرض أن $n = \prod_{i=1}^{r} p_i$ ، حيث p_i أعداد أولية . إذاً يمكن التعبير عن كل p_i كمجموع أربعة مربعات حسب مبرهنة (٧-٤-٨) وبإستخدام قضية (٧-٤-٧) يمكن التعبير عن حاصل ضرب أي عددين أوليين كمجموع أربعة مربعات . إذاً بالأستقراء على r وتطبيق قضية (٧-٤-٧) ، r من المرات يمكن التعبير عن n كمجموع أربعة مربعات .

□

<u>مثال (٧) :</u>

(أ) $12 = 3^2 + 1^2 + 1^2 + 1^2$.

(ب)

$$\begin{aligned}
513 &= 3^3 \cdot 19 = 3^2 \cdot 3 \cdot 19 \\
&= 3^2 (1^2 + 1^2 + 1^2 + 0^2)(4^2 + 1^2 + 1^2 + 1^2) \\
&= 3^2 \Big[(4+1+1+0)^2 + (1-4+1-0)^2 \\
&\qquad + (1-1-4+0)^2 + (1+1-1-0)^2 \Big] \\
&= 3^2 (6^2 + 2^2 + 4^2 + 1^2) = (3 \cdot 6)^2 + (3 \cdot 2)^2 + (3 \cdot 4)^2 + (3 \cdot 1)^2 \\
&= (18)^2 + 6^2 + (12)^2 + 3^2
\end{aligned}$$

وأخيراً نود أن نذكر تخمين ديوفنتس الذي ينص على أنه " **إذا كان** $n = 8n + 7$ ، **فلا يمكن التعبير عن n كمجموع ثلاثة مربعات** " والذي أثبت من قبل الفرنسي ديكارت (١٥٩٦-١٦٥٠) سنة ١٦٣٨م .

ويقال أن فيرما هو أول من ذكر أنه يمكن التعبير عن عدد صحيح a كمجموع ثلاثة مربعات إذاً وإذا فقط كان $a \neq 4^n(8m+7)$ ، حيث $m,n \in Z^+$. وقد أثبت ذلك كل من لجندر سنة ١٧٩٨م وجاوس سنة ١٨٠١م .

هذا وقد خمّن الإنجليزي وارنج (١٧٣٤-١٧٩٨م) سنة ١٧٧٠م أن : **أي عدد طبيعي يمكن التعبير عنه كمجموع أربعة مربعات أو تسعة مكعبات أو تسعة عشر عدداً من القوة الرابعة (Biquadratic)** . وبرهن ذلك من قبل الألماني هلبرت (١٨٦٢-١٩٤٣) سنة ١٩٠٩م .

تمارين

(١) عبر عن كل من الأعداد الآتية كمجموع مربعين 137 , 257,433,641 .

(٢) عبر عن كل من الأعداد الآتية كمجموع مربعين 26,564,725,25493 .

(٣) عبر عن العدد 85 كمجموع مربعين بطريقتين مختلفتين ، ثم عبر عن 25 كمجموع مربعين وعن 2125 كمجموع مربعين بأربعة أشكال مختلفة .

(٤) " الخازن "

(أ) إذا أنقسم عدد طبيعي إلى مربعين بشكلين مختلفين ، فأثبت أن مربعه ينقسم إلى مجموع مربعين بأربعة أشكال مختلفة .

(ب) عبر عد العدد 65 كمجموع مربعين بشكلين مختلفين ، ثم عبر عن مربعة كمجموع مربعين بأربعة أشكال مختلفة

(٥) عبر عن كل من العددين 65,85 كمجموع مربعين بشكلين مختلفين ثم عبر عن حاصل ضربهما كمجموع مربعين بستة أشكال مختلفة .

(٦) (أ) " الخازن " إذا أمكن التعبير عن عدد زوجي كمجموع مربعين ، فأثبت أنه يمكن التعبير عن نصفه كمجموع مربعين .

(ب) عبر عن 400 كمجموع مربعين ، ثم عبر عن كل من 200,100,50,25 كمجموع مربعين .

(٧) (أ) أوجد خمسة أعداد أولية يمكن التعبير عن كل منها بالشكل $n^2+(n+1)^2$.

(ب) أوجد خمسة أعداد أولية يمكن التعبير عن كل منها على الشكل 2^2+p^2 ، حيث p عدد أولي .

(٨) (أ) أثبت أنه يمكن التعبير عن 2^n كمجموع مربعين لكل $n \in N$.

(ب) إذا كان $m = 2^n \cdot a^2 b$ ، $n \geq 0$ ، a عدد صحيح فردي وكل قاسم أولي من قواسم b على الشكل $4k+1$ ، فأثبت أنه يمكن التعبير عن m كمجموع مربعين .

(ج) عبر عن كل مما يأتي كمجموع مربعين 3185 ، $2^3 \cdot 5 \cdot 11^2 \cdot 13$.

(٩) عبر عن كل من الأعداد الآتية كمجموع أربعة مربعات 231,391,2109,6543 .

(١٠) أوجد ثلاثة أعداد أولية تحقق العلاقة $p = n^2+(n+1)^2+(n+2)^2$ ، $n > 0$.

****

الفصل الثامن

الكسور المستمرة
Continued Fractions

إن أقدم معرفة للكسور الأعتيادية أو الأعداد النسبية ، تنسب إلى البابليين والمصريين فقد أوجد البابليون كسوراً على أساس النظام الستيني : نصف = 30 ، ثلث = 20 ، ربع = 15 .

وكان للمصريين ترقيم للكسر العادي $\frac{1}{4}$، $\frac{1}{6}$، $\frac{1}{21}$، $\frac{1}{98}$ ، وقد جعلوا علامة بيضوية فوق العدد للدلالة على الكسرة نحو ١١١ إلى ثلث وفي أيام أحمر كانوا يكتبون الثمن هكذا $\frac{\cdot}{-}$ ويكتبون واحد إلى عشرين هكذا $\frac{\cdot}{\wedge}$.

ووصف الخوارزمي الكسور على أساس النظام الستيني ووصف عمليات الضرب والقسمة لها بطرق مشابهة لطرق البابليين والمعروفة للإغريق ، ثم ينتقل إلى استخراج الجذر التربيعي .

أما البوزجاني (٩٤٠-٩٩٨م) فقد تناول نظرية الكسور في كتابه " فيما يحتاج إليه الكُتّاب من علم الحساب " مميزاً بين ثلاثة أنواع من الكسور الأعتيادية أو العادية وهي الكسور الرئيسية ذات الصورة التي تساوي واحد وهي من نصف إلى عشر والكسور المركبة وهي على الصورة a إلى b ، حيث $a < b \leq 10$ والكسور الوحدية وهي حاصل ضرب الكسور الرئيسية .

ويسمى أبو الوفاء الكسور الرئيسية والكسور الحاصلة من جمع أو ضرب الكسور الرئيسية " الكسور الناطقة " أما الكسور الأخرى فيطلق عليها أسم الكسور الصماء .

هذا وقد كتب الهندي ليلافتي عام ١١٥٠م الكسر الأعتيادي بالشكل $\frac{a}{b}$ جاعلاً البسط " الصورة " أعلى والمقام أسفل ، أما العدد الكسري المكون من كسر وعدد صحيح فيكتب بالشكل $\begin{matrix} a \\ b \\ c \end{matrix}$ فالشكل $\begin{matrix} 4 \\ 2 \\ 3 \end{matrix}$ يعني أربعة وثلثين ، ويعود الفضل إلى المسلمين في تطوير الكسر الأعتيادي ، والعدد الكسري فقد أدخل ابن البناء المراكشي (١٢٥٦-١٣٢١م) الخط الفاصل بين البسط والمقام فيكتب الكسر $\frac{a}{b}$ بالشكل $\frac{a}{b}$ ، وعبر عن العدد الكسري $\begin{matrix} a \\ b \\ c \end{matrix}$ بالشكل $a\frac{b}{c}$ ، ونجد في حساب ابن البنا المراكشي ، وأبو الحسن القصادي (١٤١٢-١٤٩٦م) أنماط من الكسور الأعتيادية كالكسر المنتسب مثل خمسة أتساع وأربع أسباع التسع وثلث سبع التسع وثلاثة أرباع ثلث سبع التسع أي $\frac{475}{756}$ ، والكسر المختلف مثل سبعة أتساع وثلثين وأربعة أخماس الثلث أي $\frac{77}{45}$ ، والكسر المبعض أو كسر الكسر مثل ثلث من أربعة أخماس من ستة أسباع أي $\frac{24}{105}$ أو $\frac{8}{35}$.

أما بالنسبة للكسور العشرية فإن إجراء عمليات حسابية بواسطة كسور عادية مقامها من قوى العشرة يؤكد وجود تطبيق للكسور العشرية دون الأعتراف بها ككسور ، ومنذ القرن العاشر وربما قبل ذلك نجد في مختلف الأبحاث الحسابية العربية قاعدة لتقريب الجذر الأصم (التربيعي ، التكعيبي ، ...) تسمى قاعدة الأصفار وردت في بحث للسموأل المغربي أسمه التبصرة في علم الحساب صيغتها العامة هي :

$$r=1,2,\cdots \text{ ، } a^{\frac{1}{n}}=\frac{(a\times 10^{nr})^{\frac{1}{n}}}{10^{r}}$$

والتقريب الحاصل حسب هذه القاعدة يشمل بالضرورة الكسر العشري ، ولهذا أدخل جورج سارتون إلى تاريخ الكسور العشرية كل من أجرى تطبيقاً لهذه القاعدة مثل أبو الحسن أحمد بن إبراهيم الأقليديسي الذي أورد قاعدة الأصفار عام ٩٥٢م في الحالات الخاصة للجذر التربيعي للعدد (٢) في كتابه " **الفصول في الحساب الهندي** " ، وابن طاهر البغدادي المتوفي (١٠٣٧م) في " **التكملة في الحساب** " ، لكن الدراسات التاريخية الحديثة تؤكد أن الكسور العشرية التي لا يزال ابتكارها ينسب إلى الكاشي يجب أن تكون من عمل جبريي القرنين الحادي والثاني عشر للميلاد أي إلى مدرسة الكرخي والسموءل ، ففي بحث للسموءل " **القوامي في الحساب الهندي** ، ١١٧٢م " يوجد عرض للكسور العشرية أعد في سياق مسألة أستخراج الجذر النوني للعدد ، إضافة إلى مسائل التقريب ، وقد سمى المرتبة التابعة لمرتبة الآحاد مرتبة أجزاء العشرات والتالية لها أجزاء المئات والتالية لها أجزاء الألوف وهكذا ...

ونود أن نشير إلى أن افتراض السموءل $10^0 = 1$ ووضع المتتاليتين :

$(10, 10^2, \cdots)$ ، $(\frac{1}{10}, \frac{1}{10^2}, \cdots)$ على جانبي 10^0

أي $\cdots, \frac{1}{10^2}, \frac{1}{10}, 10^0, 10, 10^2, \cdots$

يعني أن لكل عدد حقيقي r تمثيل عشري (محدود أو غير محدود) هو :

$r = \sum_{k=m}^{n} q_k (10)^k$ حيث أن $m, n \in Z^+$ ، $k \in Z$.

أما عمل الكاشي ، فهو تتويج لأعمال بدأها جبريوا القرنين الحادي والثاني عشر للميلاد يحتوي على نتائجهم فقد ورد في كتابه " **مفتاح الحساب** " عرض للكسور العشرية يشكل بعداً مهماً في تاريخها وفي بحثه " الرسالة المحيطية " عن محيط الدائرة المترجم والمنشور من قبل المؤرخ الألماني لوكي يستخدم الكاشي الكسور العشرية لتقريب العدد π عن طريق إيجاد تقريب للعدد 2π بالنظام الستيني بعد تحديده لمحيط مضلع محاط بدائرة له 3×2^{28} ضلعاً ومحيطاً بالدائرة له نفس عدد الأضلاع ، وأفتراضه أن محيط الدائرة يعادل المتوسط الحسابي لمحيطي المضلعين يحصل على النتيجة الآتية :

$$2\pi = 6,16,59,28,1,34,51,46,14,50$$

ثم حول ذلك إلى النظام العشري فوجد أن :

$$2\pi = 6.2831853071795865$$

وعليه فإن :

$$\pi = 3.14159265358979325$$

مع ملاحظة أن عدد الأرقام في النظامين الستيني والعشري واحدة مما يدل على وجود تماثل بينهما ، كما يبين تطبيق الكسور العشرية بالنسبة للأعداد الحقيقية مثل π .

وأخيراً نورد أن نشير إلى أنه إذا كان الكرخي أو السموؤل أو الأقليديسي أو الكاشي مكتشف الكسور العشرية فإن ذلك يعني أن مكتشفوها هم العرب والمسلمين وليس الفلكي الرياضي الإنجليزي سيمون ستيفن (١٥٤٨-١٦٢٠م) الذي أتى بعد الكاشي بأكثر من (١٨٥) سنة .

أما الكسور المستمرة ، فيعود تاريخها إلى الإيطاليين بومبللي سنة ١٥٧٢م وكاتالدي (١٥٢٨-١٦٢٦) سنة ١٦١٣ والإنجليزي جون وايلس سنة ١٦٥٣م وأويلر ولاجرانج وجاوس ، والكسر المستمر تعبير على الشكل :

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$ ، حيث $a_i \in R$ ، $a_i > 0$ لكل $i \geq 1$

ويرمز له بالرمز $[a_0, a_2, a_2, \cdots]$ ، والكسور المستمرة منتهية وغير منتهية ، فالكسر المستمر :

$$[3,7,15,1,292] = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292}}}} = \frac{103993}{33102} = 3 \cdot 141592653019 \simeq \pi$$

كسر منتهي ، أما الكسر المستمر :

$$\frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}} = [1,1,1,\cdots]$$

فهو كسر غير منتهي ، والكسور المستمرة قد تكون بسيطة وغير بسيطة وسنركز أهتمامنا في هذا الفصل على الكسور المستمرة البسيطة ، ويضم هذا الفصل بندين ندرس فيها الكسور المستمرة البسيطة المنتهية وغير المنتهية لأنها تمثل الأعداد النسبية وغير النسبية .

٨-١ : الكسور المستمرة البسيطة المنتهية

Finite Simple continued Fractions

سنركز أهتمامنا في هذا الجزء على دراسة هذا النوع من الكسور وعلاقته بالأعداد النسبية إضافة إلى تقارباته وخواصها .

تعريف ٨-١-١ :

الكسر المستمر المنتهي هو تعبير على الشكل :

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4}}}}$$
$$\ddots$$
$$\cfrac{1}{a_{n-1}+\cfrac{1}{a_n}}$$

حيث $a_i \in R$ ، $a_i > 0$ لكل $i \geq 1$ ، وإذا كان $a_i \in Z$ ، $a_i > 0$ لكـل $i \geq 1$ فيسمى الكسر المستمر المنتهي كسراً بسيطاً منتهياً . ويرمز عادة للكسر المستمر المنتهي بالرمز $[a_1,\cdots, a_n]$ أو $\langle a_0,a_1,\cdots,a_n \rangle$.

مثال (١) :

(أ) $[1,3]=1+\frac{1}{3}=\frac{4}{3}$.

ب) $[2,3,1,3,2]=2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2}}}}=\frac{77}{34}$.

ملاحظة :

$$[a_0,a_1,\cdots,a_n]=[a_0,a_1,\cdots,a_{n-2},a_{n-1}+\frac{1}{a_n}]$$
$$=a_0+\frac{1}{[a_1,\cdots,a_n]}$$

مثال (٢) :

$$[1,3,5,2,7,2,4,6]=1+\frac{1}{[3,5,2,7,2,4,6]}=1+\cfrac{1}{3+\cfrac{1}{[5,2,7,2,4,6]}}$$

$$=1+\cfrac{1}{3+\cfrac{1}{5+\cfrac{1}{2+\cfrac{1}{7+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{6}}}}}}}=1+\cfrac{1}{3+\cfrac{1}{5+\cfrac{1}{2+\cfrac{1}{7+\cfrac{1}{2+\cfrac{6}{25}}}}}}$$

$$=1+\cfrac{1}{3+\cfrac{1}{5+\cfrac{1}{2+\cfrac{1}{7+\cfrac{25}{56}}}}}=1+\cfrac{1}{3+\cfrac{1}{5+\cfrac{1}{2+\cfrac{56}{417}}}}=1+\cfrac{1}{3+\cfrac{1}{5+\cfrac{417}{890}}}$$

$$=1+\cfrac{1}{3+\cfrac{890}{4867}}=1+\frac{4867}{15491}=\frac{15491+4867}{15491}=\frac{20358}{15491}$$

وبصورة عامة يمكن أن نبرهن ما يلي :

مبرهنة ٨-١-١ :

كل كسر مستمر منتهي بسيط يمثل عدداً نسبياً .

البرهان :

ليكن $x_n=[a_0,a_1,\cdots,a_n]$ كسراً مستمراً بسيطاً منتهياً .

سنبرهن بالأستقراء على n بأن x_n عدد نسبي . فإذا كان $n=0$ ، فإن $x_0=[a_0]=a_0$ عدد نسبي ، وإذا كان $n=1$ ، فإن

$$x_1=[a_0,a_1]=a_0+\frac{1}{a_1}=\frac{a_0a_1+1}{a}\in Q$$

إذاً المبرهنة صحيحة عندما $n=0,1$.

والآن لنفرض أن $x_m \in \mathbb{Q}$ لكل $m < n$. ولكي نثبت أن $x_{m+1} \in \mathbb{Q}$ ، لاحظ أن

$$x_{m+1} = [a_0, a_1, \cdots, a_m, a_{m+1}] = a_0 + \frac{1}{[a_1, \cdots, a_{m+1}]}$$

لكن $[a_1, \cdots, a_{m+1}] \in \mathbb{Q}$ حسب فرضية الأستقراء الرياضي . إذاً

$x_{m-1} = a_0 + \dfrac{1}{[a_1, \cdots, a_{m+1}]} \in \mathbb{Q}$ ، وعليه فإن $x_n \in \mathbb{Q}$.

□

<u>مثال (٣) :</u>

(أ) إذا كان $x = \frac{31}{11}$ ، فإن

$$x = 2 + \frac{9}{11} = 2 + \frac{1}{\frac{11}{9}} = 2 + \frac{1}{1 + \frac{2}{9}} =$$

$$= 2 + \frac{1}{1 + \frac{1}{\frac{9}{2}}} = 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{2}}} = [2,1,4,2]$$

(ب)
$$\frac{89}{21} = 4 + \frac{5}{21} = 4 + \frac{1}{\frac{21}{5}} = 4 + \frac{1}{4 + \frac{1}{5}} = [4,4,5]$$

(ج)
$$\frac{53}{7} = 7 + \frac{4}{7} = 7 + \frac{1}{\frac{7}{4}} = 7 + \frac{1}{1 + \frac{3}{4}}$$

$$= 7 + \frac{1}{1 + \frac{1}{\frac{4}{3}}} = 7 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}} = [7,1,1,3]$$

وبصورة عامة يمكن أن نبرهن ما يلي .

<u>مبرهنة ٨-١-٢ :</u>

يمكن التعبير عن أي عدد نسبي ككسر مستمر بسيط منتهي .

البرهان :

نفرض أن $\frac{a}{b} \in Q$. إذاً بالقسمة الخوارزمية نجد أن

$$a = b a_0 + r_1 \quad , \quad 0 < r_1 < b \Rightarrow \frac{a}{b} = a_0 + \frac{1}{\frac{b}{r_1}}$$

$$b = a_1 r_1 + r_2 \quad , \quad 0 < r_2 < r_1 \Rightarrow \frac{b}{r_1} = a_1 + \frac{1}{\frac{r_1}{r_2}}$$

$$r_1 = a_2 r_2 + r_3 \quad , \quad 0 < r_3 < r_2 \Rightarrow \frac{r_1}{r_2} = a_2 + \frac{1}{\frac{r_2}{r_3}}$$

....

....

$$r_{n-2} = r_{n-1} a_{n-1} + r_n \quad , \quad 0 < r_n < r_{n-1} \Rightarrow \frac{r_{n-2}}{r_{n-1}} = a_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}}$$

$$r_{n-1} = r_n a_n \Rightarrow \frac{r_{n-1}}{r_n} = a_n$$

إذاً

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\frac{r_1}{r_2}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\frac{r_2}{r_3}}}}$$

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} = [a_0, a_1, \cdots, a_n]$$

□

ملاحظة :

أن التعبير عن عدد نسبي ككسر مستمر بسيط منتهي ليس وحيداً ، لأن

$$\frac{a}{b} = [a_0, a_1, \cdots, a_n] = [a_0, a_1, \cdots, a_n - 1, 1]$$

فمثلاً $\frac{77}{34} = [2,3,1,3,2] = [2,3,1,3,1,1]$.

والآن إلى دراسة تقارب الكسور المستمرة البسيطة .

تعريف ٨-١-٢ :

يسمى $C_m = [a_0, a_1, \cdots, a_m]$ التقارب الميمي للكسر المستمر $[a_0, \cdots, a_n, \cdots]$. إذاً

$$C_0 = [a_0] = a_0 ، C_1 = [a_0, a_1] = a_0 + \frac{1}{a_0} ، C_2 = [a_0, a_1, a_2] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} ، \cdots$$

$$C_m = [a_0, a_1, \cdots, a_m] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \ddots \cfrac{}{a_{m-1} + \cfrac{1}{a_m}}}}$$

مثال (٤) :

أوجد تقاربات الكسر البسيط $[1,2,3,4,2,3]$

الحل :

$$c_0 = [1] = 1 \quad , \; c_1 = [1,2] = 1 + \frac{1}{2} = \frac{3}{2}, c_2 = [1,2,3] = 1 + \cfrac{1}{2 + \cfrac{1}{3}} = \frac{10}{7}$$

$$c_3 = [1,2,3,4] = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4}}} = \frac{43}{30}$$

$$c_4 = [1,2,3,4,2] = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}} = \frac{96}{97}$$

$$c_5 = [1,2,3,4,2,3] = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{3}}}}} = \frac{331}{231}$$

ولدراسة خواص التقارب نورد الآتي .

تعريف ٨-١-٣:

تعرف الأعداد الحقيقية p_m, q_m لكل $-2 \le m \le n$ كالآتي :

$$p_{-2} = 0 \,,\, p_{-1} = 1 \,,\, p_0 = a_0 \;,\; \cdots ,\, p_m = a_m\, p_{m-1} + p_{m-2}$$
$$q_{-2} = 1 \,,\, q_{-1} = 0 \,,\, q_0 = 1 \;,\; \cdots ,\, q_m = a_m\, q_{m-1} + q_{m-2}$$

مثال (٥) :

بما أن $[1,2,3,4,2,3] = \frac{331}{231}$ حسب (مثال ٤) . إذاً

$$p_0 = 1 \,,\, p_1 = a_1 p_0 + p_{-1} = a_1 a_0 + 1 = 1(2) + 1 = 3$$
$$p_2 = a_2 p_1 + p_0 = 3(3) + 1 = 10 \;,\; p_3 = a_3 p_2 + p_1 = 4(10) + 3 = 43$$
$$p_4 = a_4 p_3 + p_2 = 2(43) + 10 = 96 \,,\, p_5 = a_5 p_4 + p_3 = 3(96) + 43 = 331$$
$$q_0 = 1 \,,\, q_1 = a_1 q_0 + q_{-1} = 2(1) + 0 = 2 \;,\; q_2 = a_2 q_1 + q_0 = 3(2) + 1 = 7$$
$$q_3 = a_3 q_2 + q_1 = 4(7) + 2 = 30 \;,\; q_4 = a_4 q_3 + q_2 = 2(30) + 7 = 67$$
$$q_5 = a_5 q_4 + q_3 = 3(67) + 30 = 231$$

وعليه فإن $c_0 = \frac{p_0}{q_0} = 1 \,,\, c_1 = \frac{p_1}{q_1} = \frac{3}{2} \;,\; c_2 = \frac{p_2}{q_2} = \frac{10}{7} \;,\; c_3 = \frac{p_3}{q_3} = \frac{43}{30}$

$$c_4 = \frac{p_4}{q_4} = \frac{96}{67} \,,\, c_5 = \frac{p_5}{q_5} = \frac{331}{231}$$

وبصورة عامة يمكن أن نبرهن ما يلي :

مبرهنة ٨-١-٣:

إذا كان c_m تقارباً ميمياً للكسر البسيط المستمر $[a_0, a_1, \cdots]$ ، فإن

$$0 \le m \le n \text{ لكل } [a_0, a_1, \cdots, a_m] = c_m = \frac{p_m}{q_m}$$

البرهان: " بالأستقراء على m "

إذا كان $m = 0$ ، فإن $c_0 = a_0$ ، $\frac{p_0}{q_0} = \frac{a_0}{1} = a_0$ ، وعليه فإن $c_0 = \frac{p_0}{q_0}$ وإذا

كان $m = 1$ ، فإن $c_1 = [a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$ ، $\frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1}$

وعليه فإن $c_1 = \frac{p_1}{q_1}$. إذاً المبرهنة صحيحة عندما $m = 0, 1$.

والآن لنفرض أن المبرهنة صحيحة عندما $m = k$ ، إذاً

$$c_k = [a_0, \cdots, a_k] = \frac{p_k}{q_k} = \frac{a_k\, p_{k-1} + p_{k-2}}{a_k\, q_{k-1} + q_{k-2}}$$

ولإثبات صحة المبرهنة عندما $m = k + 1$ ، لاحظ أن

$$c_{k+1} = [a_0, a_1 \cdots, a_k, a_{k+1}] = [a_0, a_1, \cdots, a_{k-1}\; a_k + \frac{1}{a_{k+1}}]$$

$$= \frac{(a_k + \frac{1}{a_{k+1}}) p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}}) q_{k-1} + q_{k-2}} = \frac{(a_k\, a_{k+1} + 1)\, p_{k-1} + a_{k+1}\, p_{k-2}}{(a_k\, a_{k+1} + 1)\, q_{k-1} + a_{k+1}\, q_{k-2}}$$

$$= \frac{a_{k+1}(a_k\, p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k\, q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1}\; p_k + p_{k-1}}{a_{k+1}\; q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}$$

إذاً $c_m = \frac{p_m}{q_m}$ لكل $0 \le m \le n$.

□

مبرهنة ٨-١-٤:

ليكن $c_m = \frac{p_m}{q_m}$ تقارباً ميمياً للكسر المستمر البسيط $[a_0, a_1, \cdots]$.

(أ) $p_m q_{m-1} - p_{m-1} q_m = (-1)^{m-1}$ ، $0 \le m \le n$.

(ب) $p_m q_{m-2} - q_m p_{m-2} = (-1)^{m-2} a_m$ ، $0 \le m \le n$.

البرهان:

(أ) " بالأستقراء على m " . إذا كان $m = 0$ ، فإن

$$\text{R.H.S.} = (-1)^{-1} = -1 \text{ ، L.H.S.} = p_0 q_{-1} - p_{-1} q_0 = -1$$

إذاً الطرفان متساويان . وإذا كان $m = 1$ ، فإن

$$\text{L.H.S.} = p_1 q_0 - p_0 q_1 = (a_1 p_0 + p_{-1}) \cdot 1 - a_0 (a_1 q_0 + q_{-1})$$
$$= a_0 a_1 + 1 - a_0 a_1 = 1$$
$$\text{R.H.S.} = (-1)^0 = 1$$

إذاً الطرفان متساويان ، وعليه فإن العلاقة صحيحة عندما $m = 0,1$.

والآن لنفرض أن العلاقة صحيحة عندما $m = k$. إذاً $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$ ، ولإثبات صحة العلاقة عندما $m = k+1$ ، لاحظ أن

$$p_{k+1} q_k - q_{k+1} p_k = (a_{k+1} p_k + p_{k-1}) q_k - (a_{k+1} q_k + q_{k-1}) p_k$$
$$= -(p_k q_{k-1} - q_k p_{k-1}) = -(-1)^{k-1} = (-1)^k$$

إذاً العلاقة صحيحة عندما $m = k+1$ ، وعليه فإن العلاقة صحيحة لكل $0 \le m \le n$.

(ب) بما أن $q_m = a_m q_{m-1} + q_{m-2}$, $p_m = a_m p_{m-1} + p_{m-2}$. إذاً

$$p_m q_{m-2} - p_{m-2} q_m = (a_m p_{m-1} + p_{m-2}) q_{m-2} - p_{m-2} (a_m q_{m-1} + q_{m-2})$$
$$= a_m (p_{m-1} q_{m-2} - p_{m-2} q_{m-1})$$

لكن $p_{m-1} q_{m-2} - p_{m-2} q_{m-1} = (-1)^{m-2}$ حسب (أ) . إذاً

$$p_m q_{m-2} - p_{m-2} q_m = (-1)^{m-2} a_m$$

نتيجة :

$(p_m, q_m) = 1$ لكل $1 \le m \le n$.

البرهان :

نفرض أن $d = (p_m, q_m)$. إذاً $d \setminus (-1)^{m-1}$ حسب مبرهنة (٨-١-٤أ) .
لكن $d > 0$. إذاً $d = 1$.

□

ملاحظة :

بإستخدام الكسور المستمرة البسيطة المنتهية ، يمكن إيجاد الحل الخاص للمعادلة الديوفنتية الخطية $ax = by = 1$ ، $(a,b) = 1$ وذلك لأنه عندما $(a,b) = 1$ ، يمكننا أن نفرض أن $p_m = a , q_m = b$ ، فنجد أن $p_m q_{m-1} - p_{m-1} q_m = (-1)^{m-1}$ حسب مبرهنة (٨-١-٤أ) ، وعليه فإن

$$a q_{m-1} - p_{m-1} b = (-1)^{m-1} \qquad \dots (1)$$

وبضرب طرفي (1) في $(-1)^{m-1} \cdot c$ ينتج أن

$$a[(-1)^{m-1} c q_{m-1}] + b[(-1)^m c p_{m-1}] = c$$

وعليه فإن الحل الخاص للمعادلة $ax + by = c$ هو

$$x_1 = (-1)^{m-1} c q_{m-1} \quad , \quad y_1 = (-1)^m c p_{m-1}$$

أما الحل العام فهو $x = x_1 + bt \ , \ y = y_1 - at$ ، $t \in Z$.

مثال (٦) :

حل المعادلة $44x + 15y = 2$

الحل

بما أن $(44,15) = 1$. إذاً يوجد حل للمعادلة أعلاه حسب مبرهنة (٧-١-١) ، ولإيجاد ذلك الحل ، لاحظ أن

$$\frac{44}{15} = 2 + \frac{14}{15} = 2 + \cfrac{1}{\cfrac{15}{14}} = 2 + \cfrac{1}{1 + \cfrac{1}{14}} = [2,1,14]$$

إذاً الحل الخاص هــو $x_1=(-1)^{2-1}\cdot 2\cdot q_1 \quad , \quad y_1=(-1)^2\cdot 2\cdot p_1$. لكــن
$p_1=a_1p_0+p_{-1}=a_0a_1+1=3$ ، $q_1=a_1q_0+q_{-2}=1$ ، إذاً

$$x_1=-2\ ,\ y_1=6$$

والحل العام هو $x=-2+15t\ ,\ y=6-44t$ ، $t\in Z$.

<u>**مثال (٧) :**</u>

حل المعادلة $33x+11y=4$

<u>**الحل**</u>

بما أن $(31,11)=1$. إذاً يوجد حل للمعادلة أعلاه حسب مبرهنــة (٧-١-١)
ولإيجاده ، لاحظ أن $\frac{31}{11}=[2,1,4,2]$. إذاً الحل الخاص هو

$$x_1=(-1)^2\cdot 4\cdot q_2 \quad , \quad y_1=(-1)^3\cdot 4\cdot p_2$$

لكن

$$p_0=a_0=2 \quad , \quad p_1=a_1p_0+p_{-1}=1(2)+1=3$$
$$p_2=a_2p_1+p_0=4\cdot 3+2=14$$
$$q_0=1\ ,\ q_1=a_1q_0+q_{-1}=1(1)+0=1\ ,\ q_2=a_2q_1+q_0=4\cdot 1+1=5$$

إذاً الحل الخاص هو

$$x_1=4(5)=20\ \ ,\ y_0=-4(14)=-56$$

والحل العام هو

$$x=20+11t\ ,\ y=-56-31t\ ,\ t\in Z$$

<u>تمـــــارين</u>

(١) عبر عن كل مما يأتي كعدد نسبي :

(أ) $[-1,2,3]$ ، (ب) $[3,5,1,3]$ ، (ج) $[1,2,3,4]$

(د) $[1,7,49,7]$ ، (هـ) $[2,1,2,1,2]$

(٢) عبر عن كل من الأعداد النسبية الآتية ككسر مستمر بسيط :

(أ) $\frac{12}{5}$ ، (ب) $\frac{28}{13}$ ، (ج) $\frac{169}{17}$ ، (د) $\frac{115}{203}$

(٣) أحسب التقاربات لكل مما يأتي :

(أ) $[1,2,3,4]$ ، (ب) $[3,1,5,1,3]$ ، (ج) $[1,4,6,2,1]$

(د) $[8,1,1,2,2]$ ، (هـ) $[-2,1,1,1,1,2]$ ، (و) $[0,23,1,6,2]$

(٤) أوجد الحل العام لكل مما يأتي :

(أ) $7x+11y=25$ ، (ب) $11x-30y=29$

(ج) $23x+51y=3$ ، (د) $66x+39y=258$

(٥) (أ) إذا كان $c_m=\frac{p_m}{q_m}$ تقارباً ميمياً للكسر المستمر البسيط $[1,2,3,4,\cdots,n,n+1]$ ، فأثبت أن

$$p_n=np_{n-1}+np_{n-2}+(n-1)p_{n-3}+\cdots+3p_1+2p_0+(p_0+1)$$

" ملاحظة : أجمع العلاقات $p_0=1\,,\,p_1=3$ ، $p_m=(m+1)p_{m-1}+p_{m-2}$ لكل $m=2,\cdots,n$ "

(ب) حقق فرع (أ) بالنسبة للكسر $[1,2,3,4,5]$.

(٦) إذا كان $c_m=\frac{p_m}{q_m}$ تقارباً ميمياً للكسر المستمر البسيط $[a_0,a_1,\cdots,a_n]$ ، فأثبت أن

(أ) $q_m\geq 2^{\frac{m-1}{2}}$ " لاحظ أن $q_m=a_mq_{m-1}+q_{m-2}\geq 2q_{m-2}$ " .

(ب) $\frac{p_m}{p_{m-1}}=[a_m,a_{m-1},\cdots,a_1,a_0]$.

(ج) $\frac{q_m}{q_{m-1}}=[a_m,a_{m-1},\cdots,a_2,a_1]$.

٨-٢: الكسور المستمرة البسيطة غير المنتهية

Infinite simple continued Fractions

سنركز أهتمامنا في هذا الجزء على دراسة الكسور المستمرة البسيطة غير المنتهية ، والتي تعطي تقريباً جيداً للأعداد غير النسبية .

تعريف ٨-٢-١ :

يقال عن كسر مستمر غير منتهي $[a_0, a_1, ...]$ أنه كسر بسيط غير منتهي (Infinite simple continued Fraction) إذا كان $a_i \in Z^+$ لكل $i \geq 1$ ، $a_0 \in Z$.

مثال (١) :

كل من $e = [2,1,2,1,1,4,1,1,6,1,1,8,\cdots]$ ، $\pi = [3,7,15,1,292,1,\cdots]$ كسر بسيط مستمر غير منتهي .

ولتحديد قيمة الكسر البسيط المستمر اللانهائي ومعرفة ما هيته نورد ما يلي .

مبرهنة ٨-٢-١ :

ليكن c_m التقارب الميمي للكسر البسيط المستمر $[a_0, a_1, \cdots, a_n, \cdots]$.

(أ) $c_0 < c_2 < c_4 < \cdots$ ، (ب) $c_1 > c_3 > c_5 > \cdots$

(ج) $c_{2m+1} > c_{2m}$ لكل $0 \leq m \leq n$.

البرهان :

(أ) ، (ب) بما أن $a_m > 0$ لكل $m \geq 1$. إذاً $q_m > 0$ ، وعليه فإن لكل $m \geq 2$ نجد أن

$$c_m - c_{m-2} = (-1)^m \cdot \frac{a_m}{q_m q_{m-2}}$$

إذاً إذا كان m عدد زوجياً، فإن $m = 2r$ ، $r \in Z$ ، وعليه فإن $c_{2r} - c_{2r-2} > 0$ وهذا يعني أن $c_{2r-2} < c_{2r}$ لكل $r \geq 1$ ، وعليه فإن $c_0 < c_2 < c_4 < \cdots$

وإذا كان m عـدد فردياً ، فـإن $m = 2r+1$ ، $r \in Z$ ، وعليـه فـإن $c_m - c_{m-2} = c_{2r+1} - c_{2r-1} < 0$ ، وهذا يعني أن $c_{2r-1} > c_{2r+1}$ ، وعليـه فإن $c_1 > c_3 > c_5 > \cdots$.

(ج) بما أن $p_m q_{m-1} - q_m p_{m-1} = (-1)^{m-1}$ لكل $0 \le m \le n$ ، حسب مبرهنة (٨-١-٤أ) . إذاً $c_m - c_{m-1} = (-1)^{m-1} \cdot \frac{1}{q_m q_{m-1}}$ ، وعليـه فـإن $c_{2t} < c_{2t-1}$ لكل $t \ge 0$ ، وبالتالي فإن $c_{2r} < c_{2t+2r} < c_{2t+2r-1} < c_{2r-1}$

□

مبرهنة ٨-٢-٢ : " Continued Fraction Limit "

إذا كان c_m تقارباً ميمياً للسكر المستمر البسيط $[a_0, a_1, \cdots]$ ، فإن $\lim_{m \to \infty} c_m$ موجود .

البرهان :

بما أن $c_0 < c_2 < c_4 < \cdots < c_{2m} < \cdots < c_{2m+1} < \cdots < c_5 < c_3 < c_1$ ، حسب مبرهنـة (٨-٢-١) . إذاً c_{2n} تكـون متتابعـة متزايـدة باضـطراد (Monotonically increasing sequence) ومحددة من الأعلى بالعدد c_1 وهذا يعني أن $c_{2m} \le c_1$ لكل $m \ge 0$ ، وعليه فإن $\lim_{m \to \infty} c_{2m}$ موجود ، ولنفرض أن $\lim_{m \to \infty} c_{2m} = \alpha$ ، $c_{2m} < \alpha$. لكن c_{2m+1} تكون متتابعة متناقصة باضطراد (Monotonically decreasing sequence) ومحدده من الأسـفل بالعـدد c_0 .

إذاً $\lim_{m \to \infty} c_{2m+1}$ موجود ، ولنفرض أن $\lim_{m \to \infty} c_{2m+1} = \beta$ لكن

$$\left| c_{2m+1} - c_{2m} \right| = \frac{1}{q_{2m} q_{2m+1}} \le \frac{1}{2m(2m+1)}$$

إذاً $\lim_{m \to \infty} (c_{2m+1} - c_{2m}) = 0$ ، وعليه فإن $\alpha = \lim_{m \to \infty} c_{2m} = \lim_{m \to \infty} c_{2m} = \beta$

إذاً $\lim_{m \to \infty} c_m$ موجود .

□

وبتطبيق مبرهنة (٨-٢-٢) نورد التعريف الآتي :

تعريف ٨-٢-٢ :

إذا كان $x = [a_0, a_1, \cdots]$ كسراً بسيطاً مستمراً لا نهائياً ، فإن

$$x = \lim_{m\to\infty} c_m = \lim_{m\to\infty}[a_0, a_1, \cdots, a_m]$$

مبرهنة ٨-٢-٣ :

إذا كان $x = [a_0, a_1, a_2, \cdots]$ كسراً بسيطاً مستمراً لا نهائياً ، فإن

(أ) $a_0 = [x]$، حيث $[x]$ صحيح x .

(ب) $x = a_0 + \dfrac{1}{[a_1, \cdots, a_n, \cdots]}$

البرهان :

(أ) بما أن $c_0 < x < c_1$. إذاً $a_0 < x < a_0 + \dfrac{1}{a_1}$. لكن $a_1 \geq 1$. إذاً $a_0 < x < a_0 + 1$ ، وعليه فإن $[x] = a_0$.

(ب) $$[a_0, a_1, \cdots] = \lim_{m\to\infty}[a_0, a_1, \cdots, a_m] = \lim_{m\to\infty}\left(a_0 + \frac{1}{[a_1, \cdots, a_m]}\right)$$

$$= a_0 + \frac{1}{\lim_{m\to\infty}[a_1, \cdots, a_m]} = a_0 + \frac{1}{[a_1, \cdots, a_m]}$$

□

مثال (٢) :

إذا كان $x = [1,1,1,\cdots]$، فإن $x = 1 + \dfrac{1}{[1,1,\cdots]} = 1 + \dfrac{1}{x}$ ، وعليه فإن $x^2 - x - 1 = 0$ ، ومنها نجد أن $x = \dfrac{1+\sqrt{5}}{2}$.

مثال (٣) :

إذا كان $x = [1,2,2,\cdots]$، فأفرض أن $y = [2,2,\cdots]$ ، تجد أن

$$y = 2 + \frac{1}{[2,2,\cdots]} = 2 + \frac{1}{y}$$

وعليه فإن $y^2-2y-1=0$ ، وبالتالي فإن $y=\frac{2+\sqrt{8}}{2}=1+\sqrt{2}$.

لكن $x=1+\frac{1}{y}$. إذاً

$$x=1+\frac{1}{\sqrt{2}+1}=1+\frac{\sqrt{2}-1}{(\sqrt{2}+1)\,(\sqrt{2}-1)}=1+\sqrt{2}-1=\sqrt{2}$$

وبصورة عامة يمكن أن نبرهن ما يلي .

مبرهنة ٨-٢-٤ :

أي كسر بسيط مستمر لا نهائي يمثل عدد غير نسبي .

البرهان :

نفرض أن $x=[a_0,a_1,\cdots]$ كسر بسيط مستمر لا نهائي . إذاً $x=\lim\limits_{m\to\infty}c_m$ ، حيث $c_m=[a_0,\cdots,a_m]$. لكن $c_m<x<c_{m+1}$. إذاً

$$0<|x-c_m|<|c_{m+1}-c_m|=\left|\ \frac{p_{m+1}}{q_{m+1}}-\frac{p_m}{q_m}\ \right|=\frac{1}{q_m\,q_{m+1}}$$

وعليه إذا كان x عدداً نسبياً ، فإن $x=\frac{a}{b}$ ، $b>0$ ، $a,b\in Z$ ، وعليه فإن $0<|a\,q_m-b\,p_m|<\frac{b}{q_{m+1}}$. لكن q_{m+1} تتزايد بازدياد m . إذاً يمكن إختيار m كبيرة كبراً كافياً بحيث أن $b<q_{m+1}$ ، وعليه أن $0<|a\,q_m-b\,p_m|<1$ لكن $|a\,q_m-b\,p_m|$ عدد صحيح موجب . إذاً $0<|a\,q_m-b\,p_m|<1$ يعني وجود عدد صحيح بين الصفر والواحد وهذا يناقض مبرهنة (١-٢-١أ) . إذاً x عدد غير نسبي .

□

مبرهنة ٨-٢-٥ :

أي كسرين بسيطين مختلفين مستمرين غير منتهيين يمثلان عددين غير نسبيين مختلفين .

البرهان :

نفرض أن $[a_0,a_1,\cdots],[b_0,b_1,\cdots]$ كسرين بسيطين مستمرين غير منتهيين ، وأن $x=[a_0,a_1,\cdots]=[b_0,b_1,\cdots]$. إذاً

$$a_0+\frac{1}{[a_1,a_2,\cdots]}=b_0+\frac{1}{[b_1,b_2,\cdots]}$$

لكن $a_0=[x]=b_0$. إذاً $[a_1,a_2,\cdots],[b_1,b_2,\cdots]$ ، وبإعادة ما سبق نجد أن $a_1=b_1$ و $[a_2,a_3,\cdots],[b_2,b_3,\cdots]$. وبالأستقراء على n نجد أن $a_n=b_n$ لكل $n>0$. إذاً أي كسرين بسيطين مختلفين وغير منتهين يمثلان عددين غير نسبيين مختلفين .

□

والآن إلى المبرهنة الآتية التي تبين أن أي عدد غير نسبي يمثل كسراً بسيطاً لا نهائياً .

مبرهنة ٨-٢-٦:

يمكن التعبير بطريقة وحيدة عن أي عدد غير نسبي ككسر مستمر بسيط لا نهائي.

البرهان :

نفرض أن x_0 عدد غير نسبي ، ولنفرض أن

$$x_1=\frac{1}{x_0-[x_0]},\ x_2=\frac{1}{x_1-[x_1]},\ \ x_3=\frac{1}{x_1-[x_2]}\ \ ,\ \ldots$$

ولنفرض أن $a_0=[x_0],\ a_1=[x_1],\ a_2=[x_2],\cdots$

وبالأستقراء على m يمكن أن نفرض أن

$$a_m=[x_m]\ ,\ x_{m+1}=\frac{1}{x_m-a_m}$$

إذاً x_{m+1} عدد غير نسبي ، لأن x_0 عدد غير نسبي ، كما أن $0<x_m-a_m=x_m-[x_m]<1$ ، وعليه فإن $x_{m+1}=\dfrac{1}{x_m-a_m}>1$ ،

وبالتالي فإن الأعداد الصحيحة $a_{m+1}=[x_{m+1}]\geq 1$ لكل $m\geq 0$.

إذاً $a_1,a_2,\cdots$ متتابعة من الأعداد الصحيحة . لكن $x_m=a_m+\frac{1}{x_{m+1}}$.

إذاً $a_i>0$ لكل $i\geq 1$ ،

$$x_0=a_0+\frac{1}{x_1}=a_0+\cfrac{1}{a_1+\cfrac{1}{x_2}}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{x_3}}}$$

$$=\cdots=[a_0,a_1,\cdots,a_m,x_{m+1}]$$

سنثبت أن $x_0=[a_0,a_1,\cdots]$ ، ولإثبات ذلك لاحظ أن

$x_{m+1}=\frac{1}{x_m-a_m}=\frac{1}{t_m}$ حيث $t_m=x_m-a_m$ ، وعليه فإن

$$x_0=[a_0,a_1,\cdots,a_m,\frac{1}{t_m}]=\frac{\frac{1}{t_m}p_m+p_{m-1}}{\frac{1}{t_m}q_m+q_{m-1}}$$

إذاً إذا كان $c_m=[a_0,\cdots,a_m]$ ، فإن

$$x_0-c_m=x_0-\frac{p_m}{q_m}=\frac{\frac{1}{t_m}p_m+p_{m-1}}{\frac{1}{t_m}q_m+q_{m-1}}-\frac{p_m}{q_m}$$

$$=\frac{p_{m-1}q_m-p_mq_{m-1}}{q_m(\frac{1}{t_m}q_m+q_{m-1})}=\frac{(-1)^m}{q_m(\frac{1}{t_m}q_m+q_{m-1})}$$

وعليه فإن

$$|x_0-c_m|=\frac{1}{q_m(\frac{1}{t_m}q_m+q_{m-1})}$$

لكن $a_{m+1}=[\frac{1}{t_m}]$. إذاً $a_{m+1}\leq\frac{1}{t_m}<1$ ، وعليه فإن

$$|x_0 - c_m| < \frac{1}{q_m(a_{m+1}q_m + q_{m-1})} = \frac{1}{q_m q_{m+1}} \le \frac{1}{m(m+1)}$$

إذاً $\lim_{m\to\infty}(x_0 - c_m) = 0$ ، وعليـــه فـــإن $x_0 = \lim_{m\to\infty} c_m$ وهـــذا يعنـــي أن $x_0 = [a_0, a_1, \cdots]$. لكن إذا كان $x_0 = [a_0, a_1, \cdots] = [b_0, b_1, \cdots]$ ، فـــإن $a_i = b_i$ لكل $i \ge 0$ حسب مبرهنة (٨-٢-٥) . إذاً لكل عدد غير نـــسبي تعبيـــر وحيد ككسر بسيط مستمر لا نهائي .

□

نتيجة :

إذا كان $c_m = \frac{p_m}{q_m}$ تقارباً ميمياً للعدد غير النسبي x ، فإن $|x - c_m| < \frac{1}{q_m^2}$.

مثال (٤):

عبر عن العدد $\sqrt{2}$ ككسر بسيط مستمر لا نهائي .

الحل :

بما أن $1 < \sqrt{2} < 2$. إذاً

$$x_0 = \sqrt{2} = 1 + (\sqrt{2} - 1) \Rightarrow a_0 = 1$$

$$x_1 = \frac{1}{x_0 - [x_0]} = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1 = 2 + (\sqrt{2} - 1)$$

وعليه فإن $a_1 = 2$ ، لكن

$$x_2 = \frac{1}{x_1 - [x_1]} = \frac{1}{\sqrt{2} + 1 - 2} = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1 = 2 + (\sqrt{2} - 1)$$

إذاً $a_2 = 2$ ، وبصورة عامة نجد أن

$$x_m = \frac{1}{x_{m-1} - [x_{m-1}]} = 2 + (\sqrt{2} - 1) \Rightarrow a_m = 2$$

وعليه فإن $\sqrt{2} = [1, 2, 2, \cdots]$.

مثال (٥):

عبر عن العدد π ككسر بسيط مستمر لا نهائي .

الحل :

بما أن $\pi = 3\cdot141592653\cdots$. إذاً

$$x_0 = \pi = 3 + (\pi - 3) \Rightarrow a_0 = 3$$

$$x_1 = \frac{1}{x_0 - [x_0]} = \frac{1}{0\cdot14159265} = 7\cdot0625133\cdots \Rightarrow a_1 = 7$$

$$x_2 = \frac{1}{x_1 - [x_1]} = \frac{1}{0\cdot6251330\cdots} = 15\cdot99659440\cdots \Rightarrow a_2 = 15$$

$$x_3 = \frac{1}{x_2 - [x_2]} = \frac{1}{0\cdot99659440\cdots} = 1\cdot00341723\cdots \Rightarrow a_3 = 1$$

$$x_4 = \frac{1}{x_3 - [x_3]} = \frac{1}{0\cdot00341723\cdots} = 292\cdot63724\cdots \Rightarrow a_4 = 292$$

إذاً $\pi = [3,7,15,1,292,\cdots]$

لاحظ أن $c_3 = \frac{355}{113}$, $c_2 = \frac{333}{106}$, $c_1 = \frac{22}{7}$, $c_0 = 3$. لكـن $\frac{314}{100} < \pi < \frac{22}{7}$

إذاً $\left| \pi - \frac{22}{7} \right| < \frac{22}{7} - \frac{314}{100} = \frac{1}{350} < \frac{1}{7^2}$

والآن إلى دراسة الكسور المستمرة الدورية .

تعريف ٨-٢-٣ :

الكسر الدوري المستمر (Periodic continued Fraction) هو كسر مستمر على الشكل $[a_0, a_1, \cdots, a_m, \overline{b_1, b_2, \cdots, b_n}]$ ، حيـث $\overline{b_1, b_2, \cdots, b_n}$ يعنـي تكرار الأعداد $b_1, b_2, \cdots, b_n$ إلى ما لا نهاية . ويسمى n طول الدورة .

وإذا كان $m = 0$ فيسمى $[\overline{b_1, b_2, \cdots, b_n}]$ كسر دوري مستمر صـرف أو بحت (Purely periodic) .

لاحظ أن $[a_0, a_1, \cdots]$ كسر دوري $\Leftrightarrow$ يوجد $r \in N$ بحيث أن $a_m = a_{m+r}$

مثال (٦):

(أ) $[2,\overline{1,2,1,6}]$ كسر دوري مستمر طوله دورته 4 .

(ب) $[\overline{2,3}]$ كسر دوري مستمر طول دورته 2 ، ولمعرفة قيمة $x=[\overline{2,3}]$ لاحظ أن

$$x=[\overline{2,3}]=[2,3,2,3,\cdots]=2+\frac{1}{[3,2,3,\cdots]}$$

$$=2+\frac{1}{3+\frac{1}{[2,3,2,3,\cdots]}}=2+\frac{1}{3+\frac{1}{x}}=2+\frac{x}{3x+1}$$

وعليه فإن $x(3x+1)=2(3x+1)+x$ ومنها نجد أن $x^2=6$ وبالتالي فإن $x=\sqrt{6}$.

تعريف ٨-٢-٤ :

يقال عن عدد حقيقي غير نبسي r ، أنه من الدرجة الثانية أو ثنائي (Quadratic Irrational) ، إذا كان r جذراً لكثيرة حدود من الدرجة الثانية بمعاملات نسبية .

مثال (٧):

(أ) $\sqrt{2}\in R$ عدد غير نسبي تربيعي أو من الدرجة الثانية لأن $\sqrt{2}$ جذر لكثيرة الحدود $f(x)=x^2-2\in Q[x]$.

(ب) $r=\frac{1+\sqrt{5}}{2}$ عدد غير نسبي تربيعي ، لأن r جذر لكثيرة الحدود $f(x)=x^2-x-1\in Q[x]$.

والآن إلى المبرهنة الآتية التي توضح العلاقة بين الأعداد غير النسبية من الدرجة الثانية والكسور الدورية .

مبرهنة ٨-٢-٧ : " Periodic characterization "

إذا كان x كسراً مستمراً بسيطاً لا نهائياً ، فإن x كسر دوري إذاً وإذا فقط كان x عدد غير نسبي من الدرجة الثانية .

البرهان:

نفرض أن $x=[a_0,a_1,\cdots,a_m,\overline{b_1,b_2,\cdots,b_n}]$ ، $y=[\overline{b_1,b_2,\cdots,b_n}]$

إذاً $y=[b_1,\cdots,b_n,y]$ ، وعليه فإن $y=\dfrac{yp_n+p_{n-1}}{yq_n+q_{n-1}}$ حسب مبرهنة (٨-١-٢) ، ومنها نجد أن $q_n y^2+(q_{n-1}-p_n)y-p_{n-1}=0$.

لكن y عدد غير نسبي حسب مبرهنة (٨-٢-٤) . إذاً y عدد غير نسبي من الدرجة الثانية . لكن $x=[a_0,\cdots,a_m,y]$ ، إذاً

$x=c'_{m+1}=\dfrac{p'_{m+1}}{q'_{m+1}}=\dfrac{yp'_m+p'_{m-1}}{yq'_m+q'_{m-1}}$ لكل $m\ge 1$ حسب مبرهنة (٨-١-٢) .

فإذا كان $y=r+s\sqrt{t}$ حيث $r,s\in Q$ ، $s\neq 0$ ، t عدد صحيح موجب ليس مربعاً كاملاً ، فإن

$$x=\frac{(r+s\sqrt{t})p'_m+p'_{m-1}}{(r+s\sqrt{t})q'_m+q'_{m-1}}=\frac{a+b\sqrt{t}}{c+d\sqrt{t}}=\frac{(a+b\sqrt{t})(c+d\sqrt{t})}{c^2-td^2}$$

$$=\frac{ac-tbd}{c^2-td^2}+(\frac{bc-ad}{c^2-td^2})\sqrt{t}=u+v\sqrt{t}$$

حيث $u=\dfrac{ac-tbd}{c^2-td^2}\in Q$ ، $0\neq v=\dfrac{bc-ad}{c^2-td^2}\in Q$ ، وعليه فإن x عدد غير نسبي من الدرجة الثانية .

ولإثبات العكس نفرض أن x عدد غير نسبي يحقق المعادلة

$ax^2+bx+c=0$ ، حيث $a,b,c\in Z$ ، $a\neq 0$ ... (1)

ولنفرض أن $[a_0,a_1,\cdots]$ كسر مستمر بسيط لا نهائي للعدد x ، ولكل m نفرض أن $r_m=[a_m,a_{m+1},\cdots]$.

سنبرهن على وجود عدد منتهي من العناصر r_m ، ولإثبات ذلك ، لاحظ أن $x=[a_0,a_1,\cdots,a_{m-1},r_m]$. إذاً

$$x=\frac{p_m}{q_m}=\frac{r_m p_{m-1}+p_{m-2}}{r_m q_{m-1}+q_{m-2}} \quad \ldots (2)$$ حسب مبرهنة (٨-١-٢) .

من (1) ، (2) ينتج أن $A_m r_m^2+B_m r_m+D_m=0$ ، حيث

$A_m=a p_{m-1}^2+b p_{m-1}q_{m-1}+c q_{n-1}^2$ ،

$B_m=2a p_{m-1}p_{m-2}+b(p_{m-1}q_{m-2}+p_{m-2}q_{m-1})+2c q_{m-1}q_{m-2}$ ،

$D_n=a p_{m-2}^2+b p_{m-2}q_{m-2}+c p_{m-2}^2$ ،

$A_m,B_m,D_m\in Z$ ، $D_m=A_{m-1}$ ،

$$B^2-4A_m D_m=(b^2-4ac)(p_{m-1}q_{m-2}-q_{m-1}p_{m-2})^2$$

لكن $(p_{m-1}q_{m-2}-q_{m-1}p_{m-2})^2=1$. إذاً $B^2-4A_m D_m=b^2-4ac$

لكن $\left|x-\frac{p_{m-1}}{q_{m-1}}\right|<\frac{1}{q_m p_{m-1}}$. إذاً $|x q_{m-1}-p_{m-1}|<\frac{1}{q_m}<\frac{1}{q_{m-1}}$ ،

وعليه فإن $p_{m-1}=x q_{m-1}+\frac{s}{q_{m-1}}$ ، $|s|<1$. إذاً

$$A_m=a(x q_{m-1}+\frac{s}{q_{m-1}})^2+b(x q_{m-1}+\frac{s}{q_{m-1}})q_{m-1}+c\, q_{m-1}^2$$

$$=(a x^2+bx+c)q_{m-1}^2+2a xs+a\cdot\frac{s^2}{q_{m-1}^2}+bs$$

$$=2a xs+a\cdot\frac{s^2}{q_{m-1}^2}+bs$$

وعليه فإن $|A_m|=\left|\ 2axs+a\cdot\frac{s^2}{q_{m-1}^2}+bs\ \right|<2|ax|+|a|+|b|$. إذاً للعدد الصحيح A_n عدد محدود من الأحتمالات .

لكن $|B_m|=\sqrt{b^2-4(ac-A_m D_m)}$, $|D_m|=|A_{m-1}|$. إذاً يوجد عدد

منتهي من الثلاثيات (A_m, B_m, D_m) وهذا يعني أنه عندما تتغير m يوجد عدد منتهي من القيم إلى r_m ، وعليه يوجد $t \in N$ بحيث أن $r_m = r_{m+t}$. إذاً

$$x = [a_0, \cdots, a_{m-1}, r_m] = [a_0, a_1, \cdots, a_{m-1}, a_m, \cdots, a_{m+t-1}, r_{m+t}]$$
$$= [a_0, \cdots, a_{m-1}, a_m, \cdots, a_{m+t-1}, r_m]$$
$$= [a_0, a_1, \cdots, a_{m-1}, a_m, \cdots, a_{m+t-1}, a_m, \cdots, a_{m+t-1}, r_{m+t}]$$
$$= [a_0, \cdots, a_{m-1}, \overline{a_m, \cdots, a_{m+t-1}}]$$

وعليه فإن x كسر دوري مستمر لا نهائي .

مثال (٨):

أوجد العدد غير النسبي من الدرجة الثانية والذي يمثل الكسر البسيط المستمر $[2, \overline{3}]$.

الحل :

نفرض أن $x = [2, y]$ ، $y = [\overline{3}]$. إذاً $y = [3, y]$ ، وعليه فإن $p_0 = 3$ ، $q_0 = 1$ ، $p_{-1} = 1$ ، $q_{-1} = 0$ ، $y = \frac{3y+1}{y}$. إذاً $y^2 - 3y - 1 = 0$ ومنها نجد أن $y = \frac{3+\sqrt{13}}{2}$. لكن $x = [2, y] = \frac{y p'_0 + p'_{-1}}{y q'_0 + q'_{-1}}$ ، حيث $p'_0 = 2$ ، $q'_0 = 1$ ، $q'_{-1} = 0$ ، $p'_{-1} = 1$. إذاً

$$x = [2, \overline{3}] \frac{2(\frac{3+\sqrt{13}}{2}) + 1}{\frac{3+\sqrt{13}}{2}} = \frac{8 + 2\sqrt{13}}{3+\sqrt{13}} \cdot \frac{\sqrt{13} - 3}{\sqrt{13} - 3} = \frac{\sqrt{13} + 3}{2}$$

مثال (٩):

أوجد العدد غير النسبي من الدرجة الثانية والذي يمثل الكسر الدوري $[1, 2, \overline{2, 1}]$.

الحل :

ليكن $y=[\overline{2,1}]$ ، $x=[1,2,y]$. إذاً $y=[1,2,y]$ ، وعليه فإن $p_0=2$ ، $q_0=1$ ، $p_1=a_0a_1+1=3$ ، $q_1=1$ وبالتالي فإن

$$y=\frac{yp_1+p_0}{yq_1+q_0}=\frac{3y+2}{y+1}$$

ومنهـا نجـد أن $y^2-2y-2=0$ ، وعليـه فـإن $y=1+\sqrt{3}$. لكـن $x=[1,2,y]$ ، $p'_0=1 , q'_0=1 , p'_1=3 , q'_1=2$. إذاً

$$x=\frac{yp'_1+p'_0}{yq'_1+q'_0}=\frac{3y+1}{2y+1}=\frac{3(\sqrt{3}+1)+1}{2\sqrt{3}+3}$$

$$=\frac{3\sqrt{3}+4}{2\sqrt{3}+3}\cdot\frac{2\sqrt{3}-3}{2\sqrt{3}-3}=\frac{(3\sqrt{3}+4)(2\sqrt{3}-3)}{3}=\frac{6-\sqrt{3}}{3}$$

حل آخر :

ليكن $y=[\overline{2,1}]$ ، $x=[1,2,y]$. إذاً

$$y=[2,1,y]=2+\frac{1}{1+\frac{1}{y}}=2+\frac{y}{y+1}$$

وعليه فإن $y(y+1)=2(y+1)+y$ ومنهـا نجـد أن $y^2-2y-2=0$ ، وعليه فإن $y=\sqrt{3}+1$. لكن

$$x=[1,2,y]=1+\frac{1}{2+\frac{1}{y}}=1+\frac{y}{2y+1}=\frac{3y+1}{2y+1}$$

$$=\frac{3(\sqrt{3}+1)+1}{2(\sqrt{3}+1)+1}=\frac{3\sqrt{3}+4}{2\sqrt{3}+3}=\frac{3\sqrt{3}+4}{2\sqrt{3}+3}\cdot\frac{2\sqrt{3}-3}{2\sqrt{3}-3}=\frac{6-\sqrt{3}}{3}$$

ومن تطبيقات الجذور المستمرة إيجاد تقريب للجذور الحقيقية لمعادلـة الدرجـة الثانية ، وتوضح ذلك الأمثلة الآتية .

مثال (١٠):

أوجد الجذور الحقيقية للمعادلة $x^2 - 2x - 1$ مقربة إلى ثلاثة مراتب عشرية .

الحل :

بما أن $x^2 - 2x - 1 = 0$. إذاً $x^2 = 2x + 1$ ، وعليه فإن

$$x = 2 + \frac{1}{x} = 2\frac{1}{2+\frac{1}{x}} = 2 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{x}}} = [\overline{2}]$$

لكن $p_m = a_m p_{m-1} + p_{m-2}$ ، $p_0 = a_0$ ، $p_{-1} = 1$ ، $p_{-2} = 0$. إذاً

$p_0 = 2$, $p_1 = a_0 a_1 + p_{-1} = 5$, $p_2 = a_2 p_1 + p_0 = 2 \cdot 5 + 2 = 12$

$p_3 = a_3 p_2 + p_1 = 2(12) + 5 = 29$, $p_4 = a_4 p_3 + p_2 = 2(29) + 12 = 70$

$p_5 = a_5 p_4 + p_3 = 2(70) + 29 = 169$

وحيث أن $q_0 = 1$, $q_{-1} = 0$, $q_{-2} = 1$, $q_m = a_m q_{m-1} + q_{m-2}$. إذاً

$q_1 = a_1 q_0 + q_{-1} = 2$, $q_2 = a_2 q_1 + q_0 = 2(2) + 1 = 5$

$q_3 = a_3 q_2 + q_1 = 2(5) + 2 = 12$, $q_4 = a_4 q_3 + q_2 = 2(12) + 5 = 29$

$q_5 = a_5 q_4 + q_3 = 2(29) + 12 = 70$

وعليه فإن $c_0 = \frac{p_0}{q_0} = 2$, $c_1 = \frac{p_1}{q_1} = \frac{5}{2}$, $c_2 = \frac{p_2}{q_2} = \frac{12}{5}$, $c_3 = \frac{p_3}{q_3} = \frac{29}{12}$

$c_4 = \frac{p_4}{q_4} = \frac{70}{29}$, $c_5 = \frac{p_5}{q_5} = \frac{169}{70}$

لكن $|x - c_m| > \frac{1}{q_m^2}$ حسب نتيجة مبرهنة (٨-٢-٦) . إذاً إذا كان $q_m > 44$ ، فإن $\frac{1}{q^2} < 0 \cdot 0005$ ، وعليه فإن أي تقارب $c_m = \frac{p_m}{q_m}$ ، $q_m > 44$ يمثل تقريباً جيداً للجذر المطلوب ، إذاً $c_5 = \frac{169}{70} \simeq 2 \cdot 414$ يمثل تقريباً جيداً لجذر المعادلة $x^2 - 2x - 1 = 0$. وحيث أن مجموع الجذرين يساوي 2 . إذاً الجذر الآخر يساوي $2 - 2 \cdot 414 = 0 \cdot 414$.

مثال (١١):

أوجد الجذور الحقيقية للمعادلة $x^2+5x-1=0$ مقربة إلى مرتبة عشرية واحدة.

الحل :

بما أن $x^2+5x-1=0$. إذاً $x^2=-5x+1$ ، وعليه فإن

$$x=-5+\frac{1}{x}=-5+\frac{1}{-5+\frac{1}{x}}=-5+\frac{1}{-5+\frac{1}{-5+\frac{1}{x}}}=[\overline{-5}]$$

$$\ddots$$

إذاً $p_0=-5\,,\ p_1=26\,,\ p_2=-135\,,\ p_3=701$

$q_0=1\,,\ q_1=-5\,,\ q_2=26\,,\ q_3=-135$ ، وعليه فإن

$$c_0=-5\,,\ c_1=\frac{26}{-5}=5.2\,,\ c_2=\frac{-135}{26}=-5.192\,,\ c_3=\frac{701}{-135}=-5.2$$

إذاً $x=-5.2$. لكن مجموع الجذرين يساوي -5 . إذاً الجذر الآخر هو 0.2 .

تمـــارين

(١) حقق مبرهنة (٨-٢-١) لكل من الكسور المستمرة الآتية : $[1,2,1,1,2,1]\,,[5,1,4,3,2,1]$.

(٢) أوجد الأعداد غير النسبية التي تمثل كلاً مما يأتي : $[\overline{2,1}]\,,[2,\overline{5}]\,,[2,\overline{1,3}]\,,[5,\overline{1,10}]$.

(٣) عبر عن كل من الأعداد الآتية ككسر بسيط مستمر دوري : $\frac{1+\sqrt{13}}{2}\,,\frac{3+\sqrt{5}}{2}\,,\sqrt{5}\,,\frac{5+\sqrt{10}}{3}\,,\frac{\sqrt{30}-2}{11}$.

(٤) أوجد العدد غير النسبي من الدرجة الثانية الذي يمثل الكسر البسيط المستمر في كل من : $[\overline{1,2}]\,,[\overline{1,3}]\,,[\overline{5,12}]$.

(٥) أوجد جذور كلاً مما يأتي مقربة إلى ثلاث مراتب عشرية :

(أ) $x^2-3x-1=0$ ، (ب) $x^2-10x-1=0$.

(ج) $x^2+2x-1=0$ ، (د) $x^2-4x+2=0$.

(هـ) $x^2+x-2=0$ ، (و) $x^2-5x+2=0$.

(٦) عبر عن كل مما يأتي مقرباً إلى خمسة مراتب عشرية :

(أ) $e=[2,1,2,1,1,4,1,1,6,1,1,8,\cdots]$

(ب) $\pi=[3\,,7\,,15\,,1\,,292\,,1\,,\cdots]$

(٧) (أ) أثبت أن $[a,\overline{\frac{a}{b}}]$ جذر حقيقي للمعادلة $x^2-ax-b=0$ بشرط أن $ab\neq 0$ و a^2+4b ليس مربعاً كاملاً .

(ب) أثبت أن $[\overline{-\frac{b}{a},\frac{b}{c}}]$ جذر حقيقي للمعادلة $ax^2+bx+c=0$ ، بشرط أن $abc\neq 0$ و b^2-4ac ليس مربعاً كاملاً .

(ج) استخدم(أ،ب) لإيجاد الجذور الحقيقية لكل مما يأتي مقربة إلى مرتبة عشرية واحدة: $3x^2-6x-4=0$, $2x^2-3x+1=0$, $x^2-6x-3=0$.

(٨) إذا كان a عدداً صحيحاً موجباً ، فأثبت أن :

(أ) $\sqrt{a^2+1}=[a,\overline{2a}]$ ، (ب) $\sqrt{a^2-1}=[a-1\,,\overline{1,2(a-1)}]$ ، $a>1$

(ج) عبر عن كل مما يأتي ككسور دورية: $\sqrt{8},\sqrt{10},\sqrt{37},\sqrt{63},\sqrt{626}$

(٩) إذا كان a عدداً صحيحاً موجباً ، فأثبت أن :

(أ) $\sqrt{a^2+2}=[a,\overline{a,2a}]$ ، (ب) $\sqrt{a^2+2a}=[a,\overline{1,2a}]$

" لاحظ أن: $a+\sqrt{a^2+1}=2a+\sqrt{a^2+1}-a=2a+\dfrac{1}{a^2\sqrt{a^2+1}}$ "

(ج) عبر عن كل مما يأتي ككسر بسيط مستمر: $\sqrt{3},\sqrt{15},\sqrt{38},\sqrt{127},\sqrt{35}$

****

المراجع

المراجع العربية

١. فالح بن عمران الدوسري : نظرية المجموعات : مطابع الصفا ، الطبعة الثانية ٢٠٠١م ، توزيع : الدار السعودية للنشر والتوزيع .

٢. فالح بن عمران الدوسري : مقدمة في البنى الجبرية ، الطبعة الثانية ، توزيع : الدار السعودية للنشر والتوزيع .

٣. فالح بن عمران الدوسري : مقدمة في رياضيات الحضارة الإسلامية وتطبيقاتها، الطبعة الأولى ٢٠٠٣م، توزيع : الدار السعودية للنشر والتوزيع .

٤. رشدي راشد : "تاريخ الرياضيات العربية بين الجبر والحساب" . مركز دراسات الوحدة العربية بيروت ١٩٨٩م .

٥. رشدي راشد : التحليل الديوفنطيسي ونظرية الأعداد : موسوعة تاريخ العلوم العربية الجزء الثاني ، مركز دراسات الوحدة العربية بيروت ١٩٩٧م (٤٩١-٥٣٨) .

المراجع الأجنبية

1. A. Baker, "A Concise Introduction to the theory of Numbers" Cambridge univ.press (1984) .

2. D. M. Burton, "Elementary Number Theory" Allyn and Bacon Co. (1980) .

3. L. Dikson, "History of the theory of Numbers" Vols I , II , III, Chelsea publishing Co. (1952) .

4. G. H. Hardy and E. M. Wright, " An Introduction to the theory of Number " 5th Edition oxFord univ. press (1979) .

5. F. Lemmermeyer, "Introduction to Number theory" Inter Net (2000) .

6. M. E. Lines, "Anumber for your Thoughts" Adam Hilger (1989) .

7. Y. I. Manin and A. A. Panchishkin, " Introduction to Mondern Number Theory" 2nd Edition Springer (2005)

8. L. Moser, "An Introduction to the Theory of Numbers" Trillia Group, Indiana (1975) .

9. I. Niven and H. S. Zuckerman: "An Introduction to the Theory of Number" 4th Edition, John wiley and Sons (1980) .

10. O. Ore: "Number Theory and its History" , Dover Publications (1980) .

11. A. J. Perttofrezzo and D. R. Byrkit, " Elements of Number Theory" , Prentice Hall Inc. (1970) .

12. H. S. Rose, "A Course in Number Theory" Oxford Science Publications (1988) .

13. K. A. Rosen, "Elementary Number Theory" 4th Edition, Addison-wesley (2000) .

14. J. P. Serre, "A Course in Arithmetic" Springer International student Edition (1973) .

15. H. Starke, "An Introduction to Number Theory" MTT Press (1984) .

جدول الأعداد الأولية الأقل من 10.000

2	167	397	641	887	1171	1453	1733
3	173	401	643	97	1181	1459	1741
5	179	409	647	911	1187	1471	1747
7	181	419	653	919	1193	1481	1753
11	191	421	659	929	1201	1483	1759
13	193	431	661	937	1213	1487	1777
17	197	433	673	941	1217	1489	1783
19	199	439	677	947	1223	1493	1787
23	211	443	683	953	1229	1499	1789
29	223	449	691	967	1231	1511	1801
31	227	457	701	971	1237	1523	1811
37	229	461	709	977	1249	1531	1823
41	223	463	719	983	1259	1543	1831
43	239	467	727	991	1277	1549	1841
47	241	479	733	997	1279	1553	1861
53	251	487	739	1009	1283	1559	1867
59	257	491	743	1013	1289	1567	1871
61	263	499	751	1019	1291	1571	1873
67	269	503	757	1021	1297	1579	1877
71	271	509	761	1031	1301	1583	1879
73	277	521	769	1033	1303	1597	1889
79	281	523	733	1039	1307	1601	1901
83	283	541	787	1049	1319	1607	1907
89	293	547	797	1051	1321	1609	1913
97	307	557	809	1061	1327	1613	1931
101	311	563	811	1063	1361	1621	1933
103	313	569	821	1069	1367	1627	1949
107	331	571	823	1087	1373	1637	1951
109	337	577	827	1091	1381	1657	1973
113	347	587	829	1093	1399	1663	1979
127	379	593	839	1097	1409	1667	1987
131	353	599	853	1103	1423	1669	1993
137	359	601	857	1109	1427	1693	1997
139	367	607	859	1117	1429	1697	1999
149	373	613	863	1123	1433	1699	2003
151	379	617	877	1129	1439	1709	2011
157	383	619	881	1151	1447	1721	2017
163	389	631	883	1163	1451	1723	2027

2029	2339	2659	2927	3259	3559	3877	4177
2039	2341	2663	2939	3271	3571	3881	4201
2053	2347	2671	2953	3299	3581	3889	4211
2063	2351	2677	2957	3301	3583	3907	4217
2069	2357	2683	2963	3307	3593	3911	4219
2081	2371	2687	2969	3313	3607	3911	4229
2083	2377	2689	2971	3319	3613	3917	4231
2087	2381	2693	2999	3323	3617	3919	4241
2089	2389	2699	3001	3329	3623	3923	4243
2099	2393	2707	3011	3331	3631	3929	4253
2111	2399	2711	3019	3343	3637	3931	4259
2113	2411	2713	3023	3347	3643	3943	4261
2129	2417	2719	3037	3359	3659	3947	4271
2131	2423	2729	3041	3361	3671	3967	4273
2137	2437	2731	3049	3371	3673	3989	4283
2141	2441	2741	3061	3373	3677	4001	4289
2143	2447	2749	3067	3389	3691	4003	4297
2153	2459	2753	3079	3391	3697	4007	4327
2161	2467	2767	3083	3391	3701	4013	4337
2179	2473	2777	3089	3407	3709	4021	4339
2203	2477	2789	3109	3413	3719	4027	4349
2207	253	2791	3119	3433	3727	4049	4357
2213	2521	2797	3121	3449	3733	4051	4363
2221	2531	2801	3137	3457	3739	4057	4373
2237	2539	2803	3163	3461	3761	4073	4391
2239	2543	2819	3167	3463	3767	4079	4409
2243	2549	2833	3169	3467	3769	4091	4421
2251	2551	2837	3181	3469	3779	4093	4423
2267	2557	2843	3187	3491	3793	4093	4441
2269	2579	2851	3191	3499	3797	4099	4447
2273	2591	2857	3203	3511	3803	4111	4451
2281	2593	2861	3209	3517	3821	4127	4457
2287	2609	2879	3217	3527	3823	4129	4463
2293	2617	2887	3221	3533	3833	4133	4481
2297	2621	2897	3229	3539	3847	4139	4483
2309	2633	2903	3251	3541	3851	4153	4493
2311	2647	2909	3253	3547	3853	4157	4507
2333	2657	2917	3257	3557	3863	4159	4513

4517	4831	5167	5501	5821	6151	6473	6829
4519	4861	5171	5503	5827	6163	6481	6833
4523	4871	5179	5507	5839	6173	6491	6841
4547	4877	5189	5519	5834	6197	6521	6857
4579	4889	5197	5521	5849	6199	6529	6863
4561	4903	5209	5527	5851	6203	6547	6869
4569	4909	5227	5531	5857	6211	6551	6871
4583	4919	5231	5557	5861	6217	6553	6883
4591	4931	5233	5563	5867	6221	6563	6899
4597	4933	5237	5569	5869	6229	6569	6907
4603	4937	5261	5573	5879	6247	6571	6911
4621	4943	5273	5581	5881	6257	6577	6917
4637	4951	5279	5591	5897	6263	6581	6947
4639	4957	5281	5623	5903	6269	6599	6949
4643	4967	5297	5639	5923	6271	6607	6959
4649	4969	5303	5641	5927	6277	6619	6961
4651	4973	5309	5647	5939	6287	6637	6967
4657	4987	5323	5651	5953	6299	6653	6971
4657	4993	5333	5653	5981	6301	6659	6977
4663	4999	5347	5657	5987	6311	6661	6983
4673	5003	5351	5689	6007	6317	6673	6991
4679	5009	5381	5669	6011	6323	6679	6997
4691	5011	5387	5683	6029	6329	6689	7001
4703	5021	5393	5689	6037	6337	6691	7013
4721	5023	5399	5693	6043	6343	6701	7019
4723	5039	5407	5701	6047	6353	6703	7027
4729	5051	5413	5711	6053	6359	6709	7039
4733	5059	5417	5717	6067	6361	6719	7043
4751	5077	5419	5737	6073	6367	6733	7057
4759	5081	5431	5741	6079	6373	6737	7069
4783	5087	5437	5749	6089	6379	6761	7079
4787	5099	5441	5749	6091	6389	6763	7103
4789	5101	5443	5779	6101	6397	6779	7109
4793	5107	5449	5783	6113	6421	6781	7121
4799	5113	5471	5791	6121	6427	6791	7127
4801	5119	5477	5801	6131	6449	6793	7129
4813	5147	5479	5807	6133	6451	9803	7151
4817	5153	5483	5813	6143	6469	6827	7159

7177	7537	7867	8221	8581	8887	9227	9539	9883
7187	7554	7873	8231	8597	8893	9239	9547	9887
7193	7547	7877	8233	8599	8823	941	9551	9901
7207	7549	7879	8237	8609	8923	9257	9587	9907
7211	7559	7883	8243	8623	8929	9277	9601	9923
7213	7561	7901	8263	8627	8933	9281	9613	9929
7219	7573	7907	8269	8629	8941	9283	9619	9931
7229	7577	7919	8273	8641	8951	9293	9623	9941
7237	7583	7927	8287	8647	8963	9311	9629	9949
7243	7589	7933	8291	8663	8969	9319	9631	9967
7247	7591	7937	8293	8669	8971	9323	9643	9973
7253	7603	7949	8297	8677	8999	9337	9649	
7283	7607	7951	8311	8681	9001	9341	9661	
7292	7621	7963	8317	8689	9007	9343	9677	
7307	7639	7993	8329	8693	9011	9349	9679	
7309	7643	8009	8353	8699	9013	9371	9689	
7321	7649	8011	8363	8707	9029	9377	9697	
7331	7669	8017	8369	8713	9041	9391	9719	
7333	7673	8053	8377	8719	9043	9397	9721	
7349	7681	8059	8387	8731	9049	403	9733	
7351	7687	8069	8389	8737	9059	9413	9739	
7369	7691	8081	8419	8741	9067	9419	9743	
7393	7699	8087	8423	8747	9091	9421	9749	
7411	7703	8089	8429	8753	9103	9431	9767	
7417	7717	8093	8431	8761	9109	9433	9769	
7433	7723	8101	8443	8779	9127	9437	9781	
7451	7727	8111	8447	8783	9133	9439	9787	
7457	7741	8117	8461	8803	9137	9461	9791	
7459	7753	8123	8467	8803	9151	9463	9803	
7477	7757	8147	9501	8819	9157	9467	9811	
7481	7759	8161	9513	8821	9161	9473	9817	
7487	7789	8167	8521	8831	9173	9479	9829	
7489	7793	8171	8527	8837	9181	9491	9833	
7499	7817	8179	8537	8839	9187	9491	9839	
7507	7823	8191	8539	8849	9199	9497	9851	
7517	7829	8209	8543	8861	9203	9511	9857	
7523	7841	8219	8563	8863	9209	9521	9859	
7529	7853	8221	8573	8867	9221	9533	9871	

دليل الرموز

$\Rightarrow$	إذا كان فإن
$\Leftrightarrow$	إذا وإذا فقط
$\wedge$	و
$\vee$	أو
$\mid \; \mid$	القيمة المطلقة
$b \backslash a$	a يقبل القسمة على b
$b \nmid a$	a لا يقبل القسمة على b
$<$	أصغر من
$\leq$	أصغر من أو يساوي
$>$	أكبر من
$\geq$	أكبر من أو يساوي
N	مجموعة الأعداد الطبيعية
N^* أو Z^+	مجموعة الأعداد الصحيحة الموجبة
Z	مجموعة الأعداد الصحيحة
Q	مجموعة الأعداد النسبية
R	مجموعة الأعداد الحقيقية
C	مجموعة الأعداد المركبة
$\pi(x)$	عدد الأعداد الأولية الأقل من أو تساوي x
$\lfloor x \rfloor$	أكبر عدد صحيح أقل من يساوي x
π	رمز الضرب
Σ	رمز الجمع أو المجموع

$\equiv \pmod{n}$ أو $\equiv_n$	يطابق قياس n
$\not\equiv \pmod{n}$ أو $\not\equiv_n$	لا يطابق قياس n
$Ord_n(a)$	رتبة العدد a قياس n
$\sigma(n)$	مجموع قواسم العدد n
$\sigma^*(n)$	مجموع القواسم الفعلية للعدد n
$\tau(n)$	عدد قواسم العدد n
$\phi(n)$	دالة أويلر
$\mu(n)$	دالة موبيص
$\lambda(n)$	دالة زيتا
$\zeta(n)$	دالة ايتا أو دالة ديركلي
F_n	أعداد فيرما
M_n	أعداد مرسين
aRn	باقي تربيعي قياس n
aNn	باقي غير تربيعي قياس n
(a/p)	رمز لجندر
(a/n)	رمز جاكوبي
$<a_0,a_1,\ldots>$ أو $[a_0,a_1,\ldots]$	كسر مستمر
g.c.d(a,b) أو (a,b)	القاسم المشترك الأعظم للعددين a,b
l.c.m(a,b) أو [a,b]	المضاعف المشترك الأصغر أو البسيط للعددين a,b

دليل المصطلحات

(أ)

(ب ، ت ، ث)

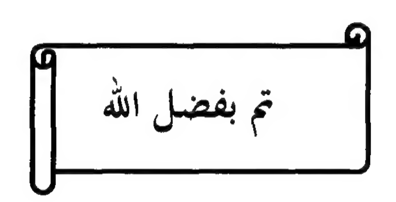
(ج ، ح ، خ)

(د)

(ر ، ز ، ش)

(ع ، غ)

(ف ، ق)


تم بفضل الله